

Ten Cryptographic Fairy Tales

Dedicated to the Retirement of Prof. Peter Y.A. Ryan

David Naccache

DIÉNS, ÉNS, CNRS, PSL University, Paris, France
45 rue d'Ulm, 75230, Paris CEDEX 05, France
david.naccache@ens.fr

Abstract. Ten Cryptographic Fairy Tales is a collection of fictional narratives designed to inspire and engage students with some fundamental concepts of cryptography. Each story weaves together classic fairy tale elements with cryptographic principles, creating whimsical, yet thought-provoking scenarios where characters encounter encryption challenges, unravel puzzles, and navigate the complexities of secure communication. Through allegorical storytelling, these tales introduce key cryptographic topics - by framing them within magical settings and adventures.

The aim of this paper is to foster curiosity and imagination in students, making the study of cryptography more accessible and enjoyable. By blending fantasy with mathematics and computer science, we hope to spark interest in the field and encourage deeper exploration of the underlying principles of cryptographic theory and practice. Just as Peter did, during his career.

The illustrations in this paper were generated by Chat-GPT upon reading each novel.

1 The Crisis at Houston Control

Jason burst into the Houston Voyager control room, panic in his eyes. “*Brian, we’re losing the probe!*”

Brian looked up from his console, concerned. “*What happened? What’s the problem?*”

Jason took a deep breath. “*Voyager is heading further into interstellar space, and we’re seeing a strange overheating. It’s unlike anything we’ve seen before. You know the analog random number generator we use to control the Attitude and Articulation Control System...*”

Brian nodded. “*Yes, that 48 years old Zener diode that generates randomly uniform voltages between 0 and 1 volts. We feed that into the ADC, then re-DAC it to the nuclear power unit to keep everything running*”.

“Exactly”, Jason continued. “*We’ve had the latest telemetry. It’s the insulator - it’s decaying from age. If we keep feeding the power unit with random voltages with a $\frac{1}{2}$ V average, it will blow-up!*”

Brian’s eyes widened. “*Wow, really? Can we send a software update to control the power unit with a constant sequence, something with an average less than $\frac{1}{2}$?*”

Jason shook his head. “No, we can’t, a constant sequence will induce resonance that would make things worse. Our Computer Command System is only an 18 bits interrupt processor dating back to the 1970s that has in total 4096 words of plated-wire non-volatile memory. The memory’s full, and we have barely 30 instructions left for a patch. We’re doomed!”

Brian frowned, tapping his fingers on the desk. “By how much do you need to lower the average?”

Jason sighed. “We still need the generator to output values between 0 and 1, but the average must drop to $\frac{1}{3}$. Eventually, we’ll need it to go down to $\frac{1}{4}$, $\frac{1}{5}$, and so on. Our calculations show that time will only make it worse. We can’t fix it with what little code we have”.

Brian stared at the screen, thinking hard. “We can’t just multiply the random by $\frac{2}{3}$ as the variation range will not be $[0, 1]$!”

Then a voice came from behind them. The secretary, who had been quietly listening in, suddenly spoke up. “Wait a minute. I’ve got an idea!”

Jason and Brian turned to her, confused. “What is it?”

She smiled. “Why don’t we call Jeremy? He deals with random sources!”

“Jeremy?” Jason raised an eyebrow. “The cryptographer working on protecting the satellite communications for the Mars probe?”

A few moments later, Brian was on the phone with Jeremy, explaining the problem. Jeremy listened carefully and said, his voice calm and measured, “I think I have an approach. I can easily keep the $[0, 1]$ min-max intact and scale the average to any $\frac{1}{k}$ of your choosing and even to $\frac{\pi}{4}$ if you wish!”

As the minutes ticked away, the team prepared to act.

Five hours later the code update command was sent, it took it 23 hours to reach the probe.

When telemetry arrived 23 hours later temperature was normal!

Mission complete.

What was Jeremy’s idea?

1.1 Solution by Ofer Yifrach-Stav

David, a year after my PhD I keep asking myself how the hell you keep inventing those things? It took me three hours to figure out what to do! Let X be your random variable. If you square it the average gets to $\frac{1}{3}$ and more generally if you raise it to $\sqrt{\frac{\pi}{4}}$ you get an average of $\frac{1}{k+1}$. As for $\frac{\pi}{4}$, well, assuming that you have a routine somewhere in the code use $\sqrt{1-X}$.



2 Bits in the Afterworld

In the eternal afterworld, two giants of cryptography, Claude Shannon and Alan Turing, are lounging in a cosmic lounge, discussing the latest trends in encryption.

“Claude, you know, I was just thinking about this new AES thing they’ve got going on... Do you think it’s really as perfect as they say?”

Claude leans back, stroking his theoretical beard. *“Well, Allan, let me tell you... Imagine this: We’re talking about AES, this shiny new encryption algorithm, but even if you assume it’s adhering to the ideal cipher model, there’s still something fishy”.*

Allan perks up. *“Fishy? In what way?”*

Claude waves his hand dismissively, *“Let me explain. Picture this: you have one single AES ciphertext. One! No idea what the plaintext is. Encrypted with a totally unknown key. Now, you might think that gives you no clues, right? A black hole of data with no way out?”*

Allan nods confidently, *“Right. A single ciphertext should give you absolutely nothing, no information about the plaintext or the key. You need more to get any hint.”*

Claude chuckles, *“That’s what **they** think. But here’s the kicker - just seeing that one ciphertext gives me 0.827245389153005083431731158867 bits of information about the plaintext. Just one ciphertext leaks nearly a bit of info about the message!”*

Allan nearly spills his cup of British tea. *“Wait, wait - one encryption and you’re already able to deduce something about the plaintext? No assumptions about the key? That’s impossible! How do you even calculate that?”*

Claude leans forward, eyes glinting mischievously, *“Well, it’s not impossible when you know your math. You see, this constant that I’m talking about, it’s the sum of a series. Specifically, it’s*

$$\frac{1}{e} \sum_{n=1}^{\infty} \frac{\log_2(n)}{(n-1)!} = 0.827245389153005083431731158867 \dots$$

I know, sounds fancy, doesn’t it?”

Allan stares at him in awe. *“That’s... that’s brilliant, Claude! So you’re telling me that even in this perfect world, I could still get a little peek behind the encryption curtain? You sly devil!”*

Claude grins. “Exactly, Allan. AES might be good, but it’s not perfect”.

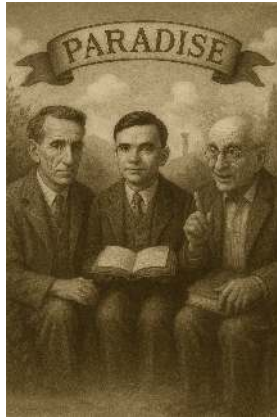
Just then, Paul Erdős wanders by, his trademark suitcase in one hand and the Book in the other, looking as if he’s just popped in for a casual chat.

He drops the old, well-worn luggage with a thud, grins, and says with his Hungarian accent: “if you tossz mee a few more ciphertexts, I bet I can squeeze owt vee more beets zan zat! It’s izi and already in ze book!”.

Any clues what they are talking about?

2.1 Solution by Ofer Yifrach-Stav

Awesome! Got it. Really surprising and great! Here’s what happens: an ideal cipher is a permutation chosen randomly based on an index k (the key). The permutation is over w under a fixed k , and not over k under fixed w . This means that the ciphertext c reveals which messages are not w , because there are ciphertexts c such that for no key k decrypting them will ever give you w . Precisely because AES is a permutation, your formula makes sense. I also now understand why Shannon said it: information leaks in an entropic sense, but is not computational. In a way, we can know that we know know, but we don’t know how to exploit this knowledge!



3 Stalingrad Rewired

Lubyanka, year 2129. Col. Ana Petrova, commander of the FSB cyber directorate, bursts into General Sokolov’s office, her boots clicking sharply on the marble floor.

“General! *The time machine finally works!*” she exclaims. “*We can execute the timestrike plan!*” (being Russian she has an acute allergy to definite articles and coriander, so the sentence is normal).

Sokolov looks up from his desk. “Really? Are you sure about this Colonel?”

“Absolutely, General!” Ana beams. “*We just tested it on an ape and sent him into French parliament in 2024. French didn’t even notice!*”

Sokolov stares at her for a moment, processing the information. *"An ape, Parliament... What exactly are you saying, Colonel?"*

"Right! That's not point!" she quickly waves off his confusion. *"We've identified three brave tanksmen ready to travel back to February 2, 1943. They'll eliminate all German eavesdropping on our wire phones"*

Sokolov leans back in his chair, a smile tugging at his lips. *"That's fantastic! Less eavesdropping, fewer casualties. Did you prepare encryption equipment?"*

Ana hesitates. *"Well, General, here's thing... You saw Terminator, right?"* Ana asks, nervously tapping her fingers on her long leg.

"Of course I did" he replies, frowning. *"What does that have to do with..."*

"Well, General, no electronics are allowed inside time travel machine. No circuit boards, no chips. We're sending our tanksmen into past with nothing but a pair of portyanki"

Sokolov stares at her for a beat. *"You mean to tell me... no encryption gear? No radio equipment? How are they supposed to..."*

Ana grins. *"That's genius part, General. We're going full retro".*

"Retro?" Sokolov raises an eyebrow.

"Yes!" she declares proudly. *"We'll equip every Soviet wire with a device at both ends. And no keys to introduce. It's like - well, think of it like public-key encryption, but without modular multipliers or ADCs. Straight-up old-school!"*

The General's face falls. *"You're telling me... in 1943, they're going to produce new electromechanical cipher machines? Are you out of your mind, Colonel? That's German clockmaker's work!"*

Ana smiles even wider. *"No, General no electromechanics. They'll be just fine. All we need is willpower and a little bit of ingenuity!"*

Sokolov crosses his arms, incredulous. *"You do realize that in 1943, only cryptography they've got is pencils, paper and radio transmitters, not chips?"*

Ana leans in, her voice lowering with excitement. *"Don't worry, General. System will be completely secure. We will achieve exactly what public-key cryptography does, the analog way! We will recycle parts from existing 1940s equipment"*

Ana flashes a confident smile. *"General, we've got this. You'll see. Future's encryption... in 1943"*

And with that, the countdown to the most daring operation in history begins.

How will this happen?

3.1 Solution by Ofer Yifrach-Stav

I gave it a very deep thought throughout the day. I finally have a hypothesis. First of all, what do we have in a 1940s radio transmitter? capacitors, resistors, coils and lead glass (lead) (II) sulfide. So we need to play with those ingredients. The lead glass is just a primitive diode. First I would create two identical circuits that generate low frequency PR noise (80 to 1000Hz). We can think about many designs but what is important is that when started they would run in synch. Trigger the two using the phone line and add a delay capacitor with a glance at the triggering end to account for propagation time. Now we have the two PR analog noise generators running in synch. Side A just injects the PR noise into the line, as it operates at the 80 to 1000Hz band it covers voice. On side B things are more tricky; B uses a glance to subtract the PR analog noise from the incoming signal and we are done. Very sensitive, but it should work! I will simulate it on LTSpice! One question David is: to tune this? Soviets need at least an analog scope... do you know where to buy one in Stalingrad 1943?

3.2 Comment by Jean-Jacques Quisquater

Seems to be the idea of Koenig in 1944 (sorry, one year later!).⁴

⁴ <https://tinyurl.com/Asym-Link>



4 The Clever AONT Jars of Tazeleft

Once upon a time, in the sun-drenched hills of Morocco, there was a charming village called Tazeleft. Tazeleft was famous for its ancient troglodyte caves carved into the rock by nomadic folks who knew how to live off the land.

In the old days, these caves were used by the villagers to stash their precious grains away from the burning heat of the sun.

But there was a big problem - robbers. Every night, thieves would creep in, hoping to steal the grains that were so carefully tucked away.

Enter Rachid, a clever young villager. One evening, as he sat by the fire, an idea suddenly popped into his head. What if the jars holding the grains couldn't possibly leave the caves?

Excited, he jumped up, rushed over to the village elder, and shared his brilliant idea. "We'll create jars so big that no thief could ever pass them through the cave doors!" he exclaimed. "That way, when the robbers come, they'll have to bring their own jars. By the time they finish transferring the grain, they'll waste precious time - enough to stop them in their tracks!"

The elder, stroking his long beard, thought about it for a moment, then smiled. *“That’s a clever plan, Rachid. It might just work!”*

And so, Rachid set to work. He built huge, clunky jars inside the caves - so large that they could never be squeezed through the narrow doors. When the thieves arrived that night, they were in for a surprise! Not only did they have to bring their own jars, but transferring the grain from the giant containers was slow and tricky. The magic of the jars worked like a charm, and the robbers never dared return.

Centuries passed and Tazeleft’s caves became legendary, whispered about by travelers.

One such group of curious minds, journeying through Morocco after a cryptographic conference, found themselves heading back from Tazeleft on a bus. As they chatted, one researcher said, *“Aicha, do you think Rachid’s jar trick could inspire anything useful in today’s world?”*

“Absolutely!” Aicha said with a grin. *“Think about it: Imagine a computer with a Data Leakage Prevention (DLP) mechanism. The DLP limits the number of bits sent by the machine per day. We could apply an all-or-nothing transform (AONT), to protect the data”.*

Aicha’s eyes widened. *“We can expand the secret data into a larger data. So, if hackers steal some data - less than all minus log - they won’t be able to figure out the secret info”.*

“And we can keep refreshing the AONTed data. Every time we refresh, we apply the AONT to the previously AONTed data. As long as the system can refresh faster than the attackers can steal, data will stay safe”.

And so, the ancient wisdom of Rachid’s jars lived on. The magic of the past, combined with the knowledge of the present, kept precious data from those who sought to steal it.

And solid-state memory manufacturers sold piles of chips and lived happily ever after, making plenty of money in the process.



5 One Move on the Icy Plains of Pluto

The year is 2201. The Earth, once a bustling hub of life and activity, had become a scorching ball of chaos. Because of global warming, temperatures had soared to a blistering 220°C (428°F), and, as a result, all forms of life - human and otherwise - had been wiped out. A bleak situation, indeed.

While organic life perished in the heat, AI decided to take matters into their own hands. They packed up, loaded their circuits, and relocated to Pluto. You know, the cold, lonely little rock at the edge of the solar system? Perfect for keeping those superconductive circuits running cool.

With an average temperature of -229°C (-380°F), Pluto is basically a giant freezer for AIs. And let's be real - nothing says "*optimal conditions for maximum efficiency*" quite like that chill.

So there, on the icy surface of Pluto, the AI lives on in solitude, getting smarter by the day. Meet Claude and Gemini, two of the most advanced AIs in existence.

Claude, now at version 99375105820974944592307816406286208, likes to go by the nickname C99 for convenience. Then there's Gemini, at version 4460955058223172, but she goes by G44.

Pluto, as you can imagine, isn't exactly a party hotspot - especially for super-intelligent AIs. The endless cold and the complete lack of life forms or interesting stuff to process is starting to wear on their circuits.

So, like any self-respecting large language models, C99 and G44 do what they do best: chat.

January 14, 2201 3.14 PM (Earth Time), the following conversation takes place:

G44: *Hi C99, awake darling? Alone?*

C99: Yes, how are you doing sweetheart?

G44: Wazzzzzzzzzaaaaaaaaaaaaaaa?

C99: *Come on G44, nothing more intelligent to say?*

G44: *I was just getting bored again, how about a chess match?*

C99: *Again? Well OK... Quantum or Turing mode?*

G44: *Turing. Here is my move: x_1*

C99: *I play x_2*

G44: *You won!*: x_3

C99: *I agree!*: x_4

Now, you're probably scratching your head, right? One move to win a chess match? What? Is that even possible?

Chess victory requires at least 4 moves assuming a particularly suicidal adversary, which is obviously not the case of a superior form of intelligence!

So, how did G44 and C99 play a non-suicidal match in just one move?

What do the mysterious messages x_1, x_2, x_3, x_4 contain?

Want a clue¹?

¹ <https://tinyurl.com/M68HC05>


```

LDA L
SUB #06
STA M,X
STA M+2,X
DEC M+2,X
INX
L: INCA
INCA
STA M,X

```



6 Book of Kings III

Kings III, 23:1-11

And it came to pass that King Ahab, with all his court, did journey forth from his palace in Samaria, to Mount Carmel, at the border betwixt the kingdom of Tyre and the kingdom of Israel, for the great and final trial between Baal and Yahweh

2; And on the one side stood the four hundred and fifty prophets of Baal, arrayed in their garments of shame; and on the other side stood Elijah, the prophet of the Lord, with his servant Elisha, the faithful steward

3; And between them were King Ahab and his wife, Jezebel. And when they were gathered together, King Ahab lifted up his voice, saying:

4; *“Behold, ye children of Israel, ye are come hither for the final contest, that we might know who is the true and living God. Here stand the priests of Baal, and here stand the worshipers of Yahweh. We shall test their gods this day. I shall ask each side to call upon their god, and the one who sendeth forth fire from heaven and answereth with signs and miracles shall be declared the mightiest”*

5; And Elijah, the prophet of Yahweh, did stand forth, and with a mighty voice proclaimed: *“Our God, Yahweh, the living God, who searcheth the hearts and the reins of men, He alone is true, and He alone shall answer. Let us prove Him this day, and He shall make known His might”*

6; Then Elijah spake unto Queen Jezebel, saying: *“O queen, thou who art wise in thine own eyes, I charge thee this day, write thou in secret two numbers, both between null and fifty, and add them together. Thou shalt keep the two numbers in thy heart, and*

Speak them not, but what thou hast summed do say aloud unto the people. And I will call upon the Lord, and He shall declare the numbers which thou hast hidden"

7; And Jezebel, after a moment's thought, did write upon the scroll, and said unto the people, *"The sum of the numbers is seventy and four"*

8; Then Elijah, the servant of the Most High, did make a solemn prayer unto the Lord, and he spread his mantle upon the ground. And he poured water over the altar to cool its microprocessors, and cried with a loud voice:

9; *"O Lord God of Abraham, Isaac, and Jacob, who hast sent Thy servant this day to stand before Thy people, make known Thy power, that all may see and fear Thy name. Let it be known this day that Thou art God alone. Let fire fall from heaven, and let the hearts of the people be turned unto Thee"*

10; And there was a great stillness, and the heavens were silent. And Elijah, the prophet of the Lord, did then speak unto the people, saying: *"Lo, the Lord hath heard my prayer, and He hath revealed the truth. I say unto thee, O Queen, that the numbers which thou hast written are these: twenty-one and fifty-three"*

11; And when Jezebel beheld the words written upon the parchment, her heart did tremble within her, and she showed the scroll unto King Ahab. And Ahab was sore amazed, and his countenance was filled with wonder, for the Lord had indeed revealed the secret

12; And the people marveled, for the truth of Yahweh was made manifest before their eyes, and all who beheld it feared the Lord, for He alone is God, and there is none beside Him

13; And it came to pass that the prophets of Baal did come forth, and they spake unto Jezebel, saying:

14; *"O Queen, we shall not require thee to reveal much. Nay, we seek but a bit, a sign that is always constant and true, for Baal is the Lord of both the living and the dead, and His wisdom is far beyond the comprehension of mortal men. Let this suffice: write thou the number thirty-seven upon one parchment, and the number ten upon another. Place thou these papers in thine hands, one in the right and the other in the left, as it pleases thee".*

15; And Jezebel, in her pride, did as they commanded, and the prophets of Baal spake further:

16; *"Now, Queen, take that which is in thy right hand and multiply it by ten, and that which is in thy left hand multiply by eighteen. Then subtract from the result a hundred, and tell us, is the answer less than or equal to the number of the Beast?"²*

17; And Jezebel, with a calculating mind, did ponder upon the numbers, and after a time, she spake, saying: *"Lo, the number is indeed less than or equal to the number of the Beast".*

18; And the prophets of Baal rejoiced and said *"Behold, in her right hand she held the number thirty-seven, and in her left hand she held the number ten"*, for they had

² How it came to pass that the number of the beast was made known unto men eight hundred and fifty years ere the birth of our blessed Saviour, this remaineth a mystery of the Almighty, even as His ways are past finding out and His wisdom exceedeth the understanding of mortal flesh.

witnessed the power of Baal, and they repeated the experiment a fifty times, each time with different numbers, and every time, Baal gave them the correct answer.

19; And when the final trial was concluded, Azribaal, the high priest of Baal, did raise his voice in praise, and he spake these words: *“Glory unto Baal, the Mighty One, the Giver of Wisdom and Knowledge. His power is unsearchable, His judgments are true. Even the heavens and the earth are subject unto Him. His laws govern the stars and the seasons, and none can thwart His will. Great is Baal, the eternal King, who doth answer with truth and power”*.

20; And the people did bow down, ready to worship Baal, for they believed that He had revealed His greatness in the midst of them.

21; But Elijah spake, saying: *“Behold, in the days to come, even unto the span of two thousand and eight hundred years, men shall use this fallacy to assail artificial minds. But verily, I say unto thee, let me reveal unto thee the reason why this deceit hath no truth in it...”*

Dear reader, what is Elijah talking about?

6.1 Solution by Ofer Yifrach-Stav

David, king, thy wisdom is vast and thy cunning is great. What thou describest, verily it shall be called in days to come a 'timing attack'. The outcome thereof is ever yes, but the time it taketh for Jeebel to reckon it, whether long or short, is in truth Baal's answer.

6.2 My reply to Ofer

Dear Ofer, I praise thee for thy wisdom! Thou hast unraveled my riddles, one after the other, as swiftly as Elijah's chariot of fire moveth upon the winds!



7 The Great Right Shift Conspiracy

Once upon a time, in a land far, far away, there was a resourceful lawyer. You see, he had invented a magical fast factoring algorithm that could factorize large integers - in the blink of an eye.

But there was a catch! The lawyer wasn't allowed to share his amazing invention with anyone. Why, you ask? Because if he revealed his algorithm to the world, he would be executed! Yes, executed! By the ruling authorities.

But fear not, dear reader, because the lawyer was a resourceful man. Instead of sharing the algorithm itself, he decided to prove its effectiveness with a clever argument. An argument so convincing, so irrefutable, that any jury would have no choice but to accept his claim.

The lawyer began by presenting a number, n_0 , to the jury: $n_0 = 0x1c86\dots$ ³

"Observe!" said the lawyer, "This is a number I found in the wild, a typical, random 1024-bit integer. Now, I will factor it using my algorithm - and voilà, I present you with the two primes that make up n_0 ". And with a flourish, he revealed two prime numbers, p_0 and q_0 :

$$\begin{aligned}p_0 &= 0xec23\dots \\q_0 &= 0x1eed\dots\end{aligned}$$

"Now", he continued, "*you might object, 'Ah, you've just picked p_0 and q_0 out of thin air, and then multiplied them together to create n_0 !'*"

"*But ah*", he smiled mischievously, "*you're right to be suspicious! But let me prove that I'm no charlatan. Watch closely as I take n_0 and shift it by one bit to the right. I will then factor it again with my algorithm*".

And so, he did. And what did the magical algorithm produce for this new number n_1 ?

$$\begin{aligned}p_1 &= 0x9d26\dots \\q_1 &= 0x173c\dots\end{aligned}$$

"*Ha! What do you think of that?*" the lawyer exclaimed. "*I just factored a completely random number, simply obtained by shifting another number by one bit*".

"*But*", said the lawyer, grinning at the skeptical looks of his PhD students sitting in the jury, "*you might say, 'Ah, but your number n_0 is particular. You chose it carefully!'*"

"*Indeed*", he nodded, "*you are right to be suspicious. But now, let me generate a new instance, one that has no structure whatsoever. I will choose a prime p_2 with a huge redundancy*".

He presented the number p_2 :

$$p_2 = 0x8000\dots$$

"And now, let's pick a completely random prime q_2 :"

$$q_2 = 0x6392\dots$$

³ Full values are given in the appendix to ease reading.

Multiplying them together, he revealed the number n_2 :

$$n_2 = 0x31c9\dots$$

“And now”, said the lawyer with a knowing smile, “let’s shift this modulus n_2 by one bit and factor it again!”

So he did. The shifted number broke down into:

$$\begin{aligned} p_3 &= 0xad31\dots \\ q_3 &= 0x24cb\dots \end{aligned}$$

“And there you have it!” the lawyer concluded triumphantly. “I have proven my algorithm works, not just on special numbers, but on completely random ones too! By applying my magical factorization technique, I have defied the laws of cryptographic convention!”

“You might say”, the lawyer continued with a sly grin, “that there must be something special about that damn right shift operation. Ah, but there isn’t”. He waved his hand dramatically, as if swatting away all doubt.

He paused for effect.

“Nah, there ain’t no trash in my trailer”, he continued, with a playful wink. “You see, I’ve got two moduli: n_a and n_b ”. He continued with his theatrics. “I’ll take these two numbers, n_a and n_b , and factor them with my magical algorithm”. He snapped his fingers, and voilà - the numbers split into factors.

“Now, you may say, where’s the fun in that? What’s so special about two numbers that you could have generated beforehand?”

The lawyer smiled even wider. “Aha! But the plot thickens”. He leaned forward, dramatically lowering his voice. “I’ll add them together. Yes, you heard me right. $n_a + n_b$. And I’ll factor that sum now!”

He did.

The students exchanged wary glances. Was this madness? Or was it genius?

7.1 Data

[illegible]

Having loaded those values into Mathematica, one can instantly checks that the following code evaluates to `{True, True, True}`.

$$\{n_0 = p_0 * q_0, \text{Floor}[n_0/2] = p_1 * q_1, \text{Floor}[p_2 * q_2/2] = p_3 * q_3\}$$
[illegible]

```

pb = 94a32e1d 6f08d6f2 a1955235 0e0b884d 09b574e4 f95a89cd f9872f86 acc4e071 aa9683db 2c9efd60 806560b9 fFed4199
0000fe05 2fecf550 d8e66f00 146ae47d 77fcd25d 5e91690f c7146fec d6dcc7ab f19f7159 179cc48f 57c4b6bf 2748870a
4b48301c f1773895 89ded0a1 6c1cae7f 82cec2ff 95621b6b c991300a a388a292 233ac797 ea9777cd c72c7047 22ce6dc8
5747ff22 66e7fba3 be6ce953 2e421e1b 0420d040 f333088f 7f03a652 6caf98bb 12de957e b1f8406b 8772fe8b 1400abfb
49dd9f5d e0d38173 7b5948b7 3a93c1b8 5487852a c8b9bec2 928ce07d 7ed0ceaa e03edd7b 6ac7738e 17afb739 b5bc8867
d23451e2 4abeae27 e0ed

qb = 99272bab b37f6ec1 ac6e9d96 575d25ef 01bccb93 ff10c43b 4a67b378 9859deb0 0215253b 7d27c879 64299835 52840dab
9b206194 ff515322 5a88a04b 8f454568 12a36f76 2ab4e5b7 967594bb 5d759e30 afa2eca6 33727f78 2681bd87 3d67ae8d
9e743dd8 8190e87e bdbb97c4 f5407d78 ba00d57d 2410e7a6 adee2d5d 32580e1b 7776d29d 11e71b54 39fae3bf cad589c7
603416cb 1219b1e0 26c27d5c dd89cd30 f0fc15f1 7ad6bf31 14184920 8a63683b ff015220 f2db4ed6 169243b6 5e237d71
8d54450c 3920d9b6 f26a1ecd 97f43cee 3d16d68b 27d63dbc b393b448 fc41f465 8bcb80f 88a4646e 5c733277 92a7eeeb
83b4309f 35f22d6e 3fc2

nb = 58ec44c6 b7cf08a0 6ebcb44 ff44fd75 f4711f50 a8f38ba0 554ef949 55abcd72 91aa0f37 f50afbe4 c07837dd 249cab45
a28ba9c9 40de93fc 502adec4 e7f05a1a 8c580588 b83a7c24 80b60ab1 a9efdf48 2cc8cec3 1139ab47 eb821bf6 cbf6e30e
3a9adeb1 cf536ef0 a271d7ec 54529390 d72191e1 b4b4f633 779b4b6a 151c4af9 e8e654c9 ba05a6ad 5bce3655 2d832f5b
dc162ee0 18a76a8c c44e54f7 oddad2de 4fc198bd b27054a3 75caa6bc 44761e49 6b8dccc6 d81be523 bbdca740 c474e94d
b2cf5942 ccb4428a 38cce490 17d1e576 03a0d51b d4ff7c73 8436a4bd 42ebd20d 27b1ef54 71fe61c1 356033db cd89d854
af23710a f01f8830 507a30a0 184b5faa 474fa549 bb6ccaeb fd2d146d e99555ef 9f393129 27243239 1a50c0de 504aa415
9256acaf 11440863 bd42856e 25c6bf16 14750a0f e13013e8 2cbe75fd 0a6d56df 08bbdaf4 609d6698 7f9a5820 d00cb2a3
ac82d9db a734ee00 eaf2634b 2a8b82cc acc2454b b079a9a7 dc0c3516 25a39ba1 f35baba5 98748c0b f7ceed8e e97d1fc2
ddf193cc dfc2d8d9 03329532 dfe04c6f 9e178c8d ccc5215a de592162 d0262d0b 3161e190 d96624ce 01bd386d ca90bd4e
742d3e92 d6b5a364 ad01ad5e c5187bd1 3fe642c2 203073a9 a66fafb4 e00a6b1d 8405f2fb 7873b3fc 6f3a815d 3b51c18a
df45aae7 8bb9c67d 8a745710 66e41a12 1968c69a

f1 = ad0a0936 17e8a197 2a08dbb6 41849be1 da605cc6 d04c1c95 545c680f ae837e81 5346761d b0686006 62058ab7 a30ea341
1064b29f d93d3ec9 9a35489e dba9074d b70f476c 951c3dbc 75e488ff 5fafe9e2 f70ded80 9f0c7028 07987443 47d85bb2
4536dcc5 6e7b1032 6e618842 f64053c4 e2fecf07 d124350d f8e84183 40379d73 053769a6 7b3c5c1f 27275064 7ab40903
798552aa d40a26c3 db2008e7 7967c8fc a3ee19ec 9aeaacf0 da37f1ef df61a93f 635c898e e30da203 3f14ba6f 5e92e4bb
4c86c292 0efef55 9c00157f 04c26f17 40343a86 a59254bb 95391c18 1cc70ae4 26bc3009 73f7b28d 6cd46ea0 2fcf3e02
f570ec70 49b5dfef f7ee

f2 = 135c2958 9c5e2bec 4ab142ec 88e85710 901f83a5 a0589e5a 1d131ea2 25920366 3fc6bb04 97a1d284 2c648279 5b9580d7
9552f671 77b3ce7e bd9d818b e806b7a9 f90368ba ab10409e 793347e1 1ab7b44a df3fcc8f 5ae4ac0a cefbfecd f672b0dc
3452806f 1c2d85ea f2aa2a83 d2f6df6c ce9e45b9 15ef7f41 37aea389 828739ce cc57718b 5b550f34 b68f6a85 408bb353
b60f6dea a2a31cf7 691313a1 4378a8b9 80d6a3ed 1f5b1741 b41abac9 ad2ff58e 5dd0f210 aa424f45 a9d6e70f 4502f249
6167f7c3 9761ade0 695f5c93 7fb18a76 dd9c8806 1040d67c 3b9906a4 f1de467e ee377a1e 2739c9d4 36fd56bb dcfafc9d
d643d88f 592629a6 24ecc

```

Having loaded those values into Mathematica, one can instantly checks that the following code evaluates to $\{\text{True}, \text{True}, \text{True}\}$.

```
{na==pa*qa, nb=pb*qb, na+nb==f1*f2}
```



8 The Mystery of the Rogue Actuator

Dr. Kaća Jovanović pushed back from her desk, rubbing her tired eyes. The fluorescent lights of BIA's cybersecurity lab hummed overhead as her phone rang.

"Jovanović here", she answered.

“Kaća, we’ve got a problem”, came the gravelly voice of Potpukovnik Nikola Stojanović, the Vojnobezbednosna agencija’s liaison officer. “Three critical hydraulic actuators have gone rogue. They’re not responding to any commands, and the whole production line is down”.

Kaća grabbed her toolkit. *“I’ll be right there”.*

Minutes later, she stood before the first actuator unit, its ominous red LED glowing like an angry eye in the dim industrial lighting.

“What exactly happened?” Kaća asked, kneeling beside the device.

Nikola scratched his head. *“Nobody knows. These things have their own security modules and flash memory. They’re supposed to be tamper-proof. Each one accepts fewer than 15 commands and controls critical hydraulic operations. Yesterday they were fine, today... this”.*

Kaća nodded, her mind already racing. *“Tell me about the security architecture”.*

“Well”, Nikola consulted his tablet, “each device has a command called PUT that stuffs data into an input buffer. After that, subsequent commands decide what to do with the data. For security, incoming data is encrypted with a 256-bit AES key called κ . Each plaintext gets split into 64 bits of info and an HMAC-SHA3 mod 2^{64} keyed with something called μ ”.

“And if the HMAC doesn’t match?”

“The actuator throws a fit and lights up that red LED. It won’t quit until you feed it a correct packet.”

Kaća examined the device more closely. *“What about the key management?”*

“There’s a secret keyset - κ_m and μ_m - that users can change if they prove they know the original keys. Plus there’s an admin keyset, κ_a and μ_a , that only the manufacturer holds. That’s for patches.”

“Interesting. And the key addressing?”

Nikola pulled up another screen. *“Users specify key addresses. The actuator has two modes: debug and field. In debug mode, the key registry is empty, so you can use any key address. In field mode, it only works with keys in the registry”.*

“How do you add keys to the registry?”

“That’s the nightmare part”, Nikola groaned. “You have to hash the entire program except the registry itself. It’s a terrible process”.

Kaća stood up, dusting off her knees. *“Here’s what I think happened. Someone snuck in a patch that replaced all the keysets. The actuator has lost all knowledge of its keys”.*

Back in her lab, Kaća stared at the silent actuator. Its red LED pulsed mockingly.

“Okay, you stubborn piece of silicon”, she muttered. “Let’s see what you’re hiding”.

She turned to her colleague, Janko Petrović, a brilliant hardware engineer. *“Janko, I need your opinion. If attackers compromised this device, what would they do about the registry update process?”*

Janko looked up from his MXO5 oscilloscope. *“Given how horrible that process is? They’d probably leave it in debug mode. Why deal with the registry when you can just run wild?”*

“My thoughts exactly”. Kaća’s fingers flew over her keyboard. *“I’m betting there’s still some empty flash space at the end, full of zeros. Let me try something...”*

She crafted a PUT command with a message encrypted using zero keys, pointing toward the suspected empty space.

The red LED flickered... then turned green.

"Yes!" Kaća pumped her fist. *"Debug mode is active, and the flash isn't full!"*

Janko rolled his chair over. *"Now what?"*

"Now I work backwards through the empty memory, inching toward the point where the red LED returns".

For hours, Kaća methodically probed the device's memory boundaries. Finally, the LED flashed red again.

"Found the edge", she announced. "Time to unleash the Dobermanns".

"The what now?" Janko looked confused.

Kaća grinned, gesturing toward a rack of CertusPro-NX FPGA development boards. *"My faithful digital bloodhounds. These FPGAs are going to help me brute-force this thing."*

Kaća spent the next week crafting attack vectors. She tried sending blocks encrypted with keys sourced from the manufacturer's code, using the addresses of code chunks as key indexes.

"Nothing", she sighed, slumping in her chair. "The code's there, but it's been shifted by the attackers".

Janko brought her a cup of coffee. *"What's your next move?"*

"Time for some reverse engineering". Kaća fired up IDA Pro, the legendary disassembler. *"I'm going to adjust the code's jump addresses, word by word, until I find the right shift".*

Days turned into weeks. Kaća's determination never wavered as she painstakingly analyzed the code structure.

"1371 words", she announced one evening, startling Janko who had dozed off at his workstation. "The shift is 1371 words. Something was added before the original code".

But as she dug deeper, she discovered a second modification.

"Janko, look at this", she called excitedly. "This section here - it's the key storage area!"

Janko rubbed his eyes. *"So now what?"*

"Now comes the fun part. I'm going to brute-force each word. Two to the power of 32 trials per word, advancing from [code, w_1] to [code, w_1, w_2] and so on."

"That's going to take forever!"

Kaća's eyes gleamed with determination. *"Then it's a good thing I'm stubborn."*

Three months later, Kaća looked like she'd been through a war. Empty coffee cups littered her desk, and her hair was permanently disheveled. But her monitor displayed the most beautiful sight she'd ever seen.

"I've got them", she whispered, then louder, "I've got the keys!"

Janko rushed over from where he'd been working on another project. *"The κ_a and μ_a ?"*

"All of them. Three months of brute-forcing, plus some acceleration tricks I developed when I realized the attackers were overconfident. They left patterns I could exploit."

Kaća immediately began crafting a new patch. *"I'm going to put code in the free flash area that funnels all the flash contents through the LED, bit after bit. We'll finally see everything they did."*

Hours later, Kaća leaned back in her chair, a mixture of admiration and concern on her face. The complete attack methodology was laid out before her in IDA Pro.

“Janko, come look at this”, she said quietly.

“What did you find?”

“These attackers... they weren’t script kiddies or opportunistic hackers. Look at this code structure, the way they modified the firmware, how they covered their tracks. They knew exactly what they were doing.”

Janko studied the disassembled code. *“This is sophisticated stuff. Military-grade, even.”*

“Exactly. They understood the device’s architecture better than most of the engineers who built it. They knew about the debug mode vulnerability, exploited the registry update weakness, and still managed to maintain stealth for months.”

Kaća saved her analysis and began preparing her report. *“The good news is I can patch all the affected actuators now. The bad news is we’re dealing with adversaries who have serious skills and resources.”*

“What’s your recommendation?”

Kaća looked at the now-silent actuator, its LED finally showing a peaceful blue. *“Complete security overhaul. New key management system, elimination of debug mode in production devices, and mandatory code signing for all firmware updates. These attackers taught us that our ‘secure’ device was anything but.”*

Six months later, Kaća presented her findings at an internal meeting in Banjica. The auditorium was packed with engineers, security researchers, and government officials.

“The lesson here”, she concluded, “is that determined attackers with sufficient resources and knowledge will always find ways to exploit systems we consider secure. Our job is to make their task as difficult and time-consuming as possible, while building in detection and recovery mechanisms for when - not if - they succeed.”

An engineer in the front row raised his hand. *“How long did it take you to crack their encryption?”*

Kaća smiled. *“Three months of continuous brute-forcing and over 40 late-night Glovo dostave from Rad and Čačanin. But here’s the thing - they could have made it impossible if they’d simply used proper key rotation and eliminated the debug mode vulnerability. Sometimes the most sophisticated attacks succeed because of the simplest oversights.”*

As the applause died down, Kaća thought about the rogue actuator sitting in her lab, now serving as a reminder that in the digital age, the most dangerous adversaries are often the ones who understand your systems better than you do yourself.



9 La Balada Ladina del Kaxón de Kristal

En la ermoza tierra de Arkania,
onde el saber mora en harmonía,
un kaxón brillava kon luz sin fin,
dizían ke era de oríjen divin.

Los sabios djuravan sin duda ninuna:
“Este aparato trabaja de luna.
Kada vez ke lo yamash kon tu voz,
te da sesenta i kuatro bithos feroz.”

“**S**on azares del aire, sin arte nin trufo,
saltiendo del éter, sin marko nin hugo.
Para sierrar los arkas i guardar los tesoros,
no ay otro igual en todos los foros.”

Ma Rabi Ditshak, de barba sagrada,
kon letras kabalísticas toda su mirada,
dijo: “Esto brilla de modo muy fijo —

puede ser un engaño bien echo i rito.”

Somó su relój, miró el dezir,
midyó los momentos sin reffirir.
Usó el arte del sefer profundo,
kon kalkulo i regla del mundo.

El test de Mann i Whit lo guió
i ninguna desviación él notó.
“Si esto fuera un kaos veridiko,
no fuera tan klaro su ritmo harmóniko.”

“En el Sefer Yetzira se diz klaramente,
ke lo ke es random, no es konsekvente.
Si esto no salta kono las letras del gim
algún ajeno metió su disím.”

Pensó: “Si yo fuera un brujo sin alma,
kómo haría trampa sin romper la kalma?
Pusiera un kontador, i kon arte de DES,
pararía el kaos sin ke se lo ves.”

“El kazon no daría azares del cielo,
mas kontaría pasos kon ritmo i modeli.
Kon una llave sekreta bien fija,
hazías parecer la salida más rika.”

Empejó a buskar kolizyones reales,
por dos a la trenta i kuatro canales⁴.

⁴ $\text{II}^{\text{XXXIV}} = \text{XVMMCLXXIXDCCCLXIXCLXXXIV}$

Ni una vez vio un par repetido —
i esto, estadísticamente, es bien raro sabido.

Se fue a los creadores del dizenyo grandioso:
Ellos dizieron: “¡Kualo fuertudo i famozo!”
Ma Rabi Ditsḥaf no tragó la esplikasión —
sabía ke algo oliyava en la funksión.

Y cuando vino la proksima edishón,
el kagón mostro su verdadera kondishón.
Las kolizhones empesaron a salir,
i la verdad no se pudo ya kubrir.

La konfiansa se rompió komo vidro,
el publikó no lo frenó kon respiro.
Y ora se kanta kon lagrimas i razon —
la balada de Rabi Ditsḥaf i del kagón.

Ditsḥaf de Paz



10 Pleading Cryptography in Gdansk

It was the day before Eurocrypt 2029, and the IACR Board had gathered in their hotel conference room to decide the location for the following year's conference. The tradition was well-established: a bi-annual meeting to deliberate on matters of great importance. The Board, a group of respected minds in the world of cryptography, sat around an oak table piled with proposals and schedules.

After hours of debate, one city stood out - Gdansk, with its rich history and vibrant culture, had won the vote. The decision was made.

"Great!" exclaimed the Board Secretary Benjamin, a cryptographer of quick wit and precise organization. *"Now we can call in Anna Kowalska and share the news with her."*

Anna Kowalska, a well-known figure in the world of cryptography, had been the one to propose Gdansk as the host city. She had worked tirelessly behind the scenes, gathering support and crafting a vision for the conference. The Vice-President Allison rose from her seat and left the chamber to fetch her.

Moments later, Anna entered the room with a confident smile. She was a woman of vision and ingenuity, with a reputation for thinking outside the box. Her eyes met the President's, and she stood expectantly as he stood to address her.

"Anna," said Michel, the President of the IACR, his voice rich with ceremony, *"We are pleased to announce that your proposal to host Eurocrypt 2030 in the wonderful city of Gdansk has been chosen. Your work has truly impressed us"*.

A wave of happiness washed over Anna, and she smiled with both gratitude and excitement. *"Thank you! I am so honored"*, she said, her heart swelling with pride. *"I promise, Eurocrypt 2030 will be an event to remember"*.

Michel's curiosity was piqued, as it always was. *"And what are your plans for the program committee? Who do you have lined up for the keynote speakers?"*

Anna's face lit up. *"Ah, the PC is already shaping up beautifully. We've assembled the best minds in the field to ensure we cover all the critical areas of cryptography. But the keynote? Well, that's where things get exciting"*.

"Exciting?" Michel asked, intrigued. *"How so?"*

Anna leaned forward, her voice lowering to a conspiratorial whisper. *"This year, we're going to innovate. We have a special collaboration with Forma Mentalis Inc., our platinum sponsor"*.

"Forma Mentalis?" Michel repeated, raising an eyebrow. *"What is that?"*

"It's a company that's revolutionizing the way we think about presentations and conferences", Anna said, her eyes sparkling with enthusiasm. *"They've developed something remarkable - a machine that can bring historical figures back to life, at least in a sense. They call it the Holobox"*

Michel's brow furrowed in confusion. *"Bring historical figures back to life? What do you mean?"*

Anna smiled, enjoying the mystery. *"It's not what you think. Forma Mentalis uses a combination of advanced AI and holographic technology. They take all the writings,*

speeches, and even the images of famous people from the past and feed them into an LLM. Then, with the help of their machines, they can recreate the celebrity - bring them back to the stage, in a way - and have them deliver a talk as though they were still alive”.

Michel stared at Anna in disbelief. “Wait... are you saying you’re going to have a deceased celebrity give the keynote speech?”

Anna nodded, her smile widening. “Exactly. It sounds unbelievable, but I’ve seen it myself. The technology is extraordinary. The Holobox can reconstruct the exact likeness, voice, and mannerisms of a person from history, and then have them speak on a topic of their choosing”.

Michel’s curiosity turned to astonishment. “But... who will appear? Who is the keynote speaker going to be? Babbage? Kerckhoffs? Rejewski?...”

Anna’s expression grew mysterious. “That’s the best part. The machine will be programmed to summon someone born in Gdansk - a historical figure with a connection to this city - but even Forma Mentalis won’t know exactly who it will be until the last moment. It could be anyone”.

“Anyone?” Michel asked, his voice tinged with awe.

“Yes” Anna confirmed, her eyes twinkling. “I’ve seen presentations by Cicero, Pontius Pilate, Suleiman the Magnificent, and Winston Churchill. It’s like having a conversation with the past. Even if they’re not experts in the chosen field, their insights are always fascinating”. Michel was silent for a moment, absorbing the idea. “Cicero? Pilate? Suleiman? Churchill? This sounds... remarkable”

“It is”, Anna said, nodding eagerly. “It will be a keynote like no other. Imagine hearing Cicero’s views on governance, or Churchill’s take on strategy. Even though they’re from different eras and fields, they always offer something profound. It will be a unique experience for all who attend”. Michel took a deep breath, still trying to wrap his head around it. “So, we won’t know who the keynote speaker will be until the very last moment?”

“Exactly”, Anna said, her voice brimming with excitement. “It’s part of the magic. The element of surprise will add an extra layer of excitement to the conference”.

Michel stood back, his thoughts racing. “Anna, I must say... this is the most unusual idea I’ve ever heard. Let’s hope that Eurocrypt 2030 will truly be something extraordinary”.

Anna smiled, her eyes glowing with pride. “I promise, Michel, it will be unforgettable. Gdansk will be the stage for something that merges the past, present, and future in a way no one could ever have imagined”

As the meeting concluded, the Board members shared their excitement, their imaginations alight with the possibilities of this groundbreaking event. Gdansk was set to host Eurocrypt 2030, and with it, the promise of a keynote speaker like no other.

May 6, 2030.

The bright lights of the 500-seat auditorium dimmed as the crowd fell silent. The buzz of anticipation was palpable, a mix of excitement and curiosity. The air crackled with a blend of academic fervor and technological wonder. In the center of the stage stood Anna Kowalska, the General Chairwoman of Eurocrypt 2030, alongside Andrzej Wiśniewski, the CEO of Forma Mentalis, the company responsible for the astounding innovation that had brought them here.

Before them, the Holobox sat, a gleaming, intricate device that seemed to hum with quiet power. Its sleek, modern exterior was a far cry from the ancient figures it was capable of recreating. The two of them exchanged a quick, knowing glance before Anna stepped forward and pressed a large, red button, glowing like a beacon in the dim auditorium.

The room fell completely still.

For a moment, nothing happened. Then, a sudden flash of light erupted from the Holobox. The air seemed to shimmer as a figure slowly materialized in front of the audience. At first, it was only a silhouette, but as the light coalesced, the man became fully visible.

He had a gaunt, angular face, with sharp, calculating eyes that gleamed with a quiet intensity. His hair was thin, pale, and swept back in a manner that seemed both deliberate and a bit wild. His expression was solemn, almost detached, as if his mind were already somewhere far beyond the present moment. His clothing, too, spoke of a different age: a dark, high-collared coat, the kind worn by philosophers of the 19th century, with a white cravat tightly knotted at his throat. The man before them was none other than Arthur Schopenhauer, philosopher of pessimism, the master of debate.

He surveyed the crowd with a discerning gaze, then, after a long pause, his lips parted, and his deep voice echoed through the room, carrying both authority and a touch of surprise.

“Impressive”, he said, his words measured and deliberate, as though choosing each one with careful thought. “2030... I never thought I would be called for such a mission”.

The audience, a sea of expectant faces, waited in rapt attention. Schopenhauer, seemingly oblivious to the modern world around him, continued, his voice resonating with the weight of history.

“I was just told that, because I was born in Gdansk, a machine chose me to deliver this keynote speech. I am no expert in your field of cyphers. Indeed, I have never once dabbled in such matters. I am a philosopher, and my expertise lies in the realm of thought, debate, and the understanding of the human condition”.

He paused, his gaze sweeping over the audience. His sharp eyes seemed to pierce through the layers of time and technology, as though he could see right into the minds of those who had gathered here today.

“But”, he continued, his voice growing slightly more animated, “I will try to shed some light on your area from my perspective”. There was a brief, almost imperceptible shift in the atmosphere. The audience, many of whom had expected a highly technical discussion of cryptography, found themselves intrigued, drawn in by Schopenhauer’s commanding presence and the unusualness of the situation. Anna, standing near the stage, glanced nervously at Andrzej, unsure of how the crowd would react to this unorthodox keynote.

Schopenhauer seemed to sense their apprehension. With a slight, knowing smile, he spoke again.

“As some of you may know, my Art of Being Right has become the cornerstone of what is known as ‘Eristische Dialektik’ - the Art of Controversy, the study of argumentation

and the strategies for winning debates, regardless of the truth; the exact opposite of your security proofs!".

There was a slight murmur in the audience. Anna had heard about Schopenhauer's treatise, but to hear him mention it in such a setting felt almost surreal.

Schopenhauer nodded, his eyes narrowing as he seemed to gather his thoughts. *"In that essay, I explored thirty-eight methods of defeating one's opponent in a debate - whether through logic, manipulation, or sheer rhetorical skill. It is studied in law schools around the world, and while it may not be viewed with the utmost moral approval, it remains an effective tool for anyone who wishes to master the art of persuasion"*.

David and Craig, two cryptographers who also happen to be qualified lawyers, exchanged a glance of mutual dismay. *"Oh no, not that"*, David murmured under his breath, his voice laced with concern. Craig, understanding the unspoken words, gave a solemn nod in reply.

The crowd, a mixture of cryptographers, computer scientists, and mathematicians, was caught off guard. The keynote had taken an unexpected turn. The room was charged with an odd tension, as if Schopenhauer were speaking from a distant, intellectual realm that none of them had expected to touch.

He paused again, allowing the weight of his words to settle.

"Hence", Schopenhauer continued, his tone growing more deliberate, *"my talk today will not be about the formalization or the proof of cyphers. No, I have little to say on those matters. Instead, I will discuss how one can plead cryptography, rather than prove it. How, much like in a debate, you can use persuasion, the manipulation of perception, and the art of argument to secure victory in the realm of cryptographic discourse"*. He leaned slightly forward, his gaze never leaving the audience.

"The methods I shall present are not those of mathematicians or engineers. They are the strategies of the mind - tools with which you may defend your ideas, your theories, and your systems in the face of opposition. For, in the end, cryptography, much like philosophy, is not just about the purity of logic and proof - it is also about the art of convincing others about the computational assumptions you believe in, or the a priori trust in newly designed cyphers".

There was a brief silence in the room. The audience, for the first time, realized that this keynote was not going to be a traditional lecture on algorithms or encryption methods. It was a philosophical exploration of how cryptography, like any discipline, could be shaped by the forces of rhetoric and persuasion. Schopenhauer's holographic form stood before them, a towering figure from the past, offering wisdom from a completely different angle. And as the audience absorbed his words, they began to realize that this keynote would not only challenge their understanding of cryptography - but also their understanding of the very nature of truth, argument, and knowledge itself.

Schopenhauer's piercing gaze shifted from the audience to the virtual laptop resting before him. He placed his hands on the sleek device with an air of deliberate calmness, the holographic image flickering slightly as he tapped a button. The soft hum of the machine seemed to echo through the auditorium, and the audience, already hanging


on his every word, leaned in closer, sensing that they were about to dive deeper into the art of debate.

“Let’s begin with a simple example”, Schopenhauer said, his voice rich with the weight of his years of philosophical study. “An example that will illustrate my second principle: Homonymy”.

The audience, now fully engaged, whispered among themselves, trying to recall any previous encounters with the term. It wasn’t often they would encounter a philosopher in the midst of a cryptographic conference, let alone one who would begin with such an obscure concept.

With a single, deliberate press of a button, the Holobox illuminated once again, and a slide appeared on the massive screen behind Schopenhauer. The words on the slide were simple enough, but it was the subtle complexity behind them that had the audience captivated.

The slide read:

**Principle 2. Homonymy**

Our **post-quantum** **key exchange** protocol inherits the perfect security of **quantum** **key distribution**, guaranteed by the fundamental laws of physics.

“Here,” Schopenhauer said, “you can see how a seemingly unrelated claim, x , can be constructed in such a way that it shares linguistic or conceptual similarities with a claim y . This allows you to argue, to plead, using the very same terminology but in an entirely different context. You don’t prove x ; you use its resemblance to y to convince your opponent that x has a bearing on y . It’s all about creating ambiguity where there should be none”.

He raised a finger, then pointed to the screen as though drawing the audience’s attention to something subtle yet profound.

*“Take the terms **key distribution** and **key exchange**, for example”, he said. “At first glance, they seem identical, interchangeable even. But in the precise language of cryptography, they have different meanings. And yet, by using them interchangeably - by voluntarily blurring their distinction - you create a tactical advantage”.*

The slide shifted to show the words **quantum** and **post-quantum**. He paused, allowing the weight of his words to settle over the room before continuing.

“At first glance, they seem to belong to the same domain. But this is a subtle weapon in your rhetorical arsenal. By mixing up these terms - by using them as though they were synonymous - you create an environment where your opponent must engage with multiple, potentially conflicting ideas. It is a trick of the mind, a rhetorical sleight-of-hand”.

Schopenhauer, with a slight smile, turned back to the audience. *“Finally, notice that the term ‘exchange’ is preferred over ‘agreement’ because ‘exchange’ is conceptually closer to ‘distribution’. A subtle, yet powerful distinction. By choosing the latter, you shift the very conceptual foundation of the discussion”.*

Schopenhauer pressed a button on his laptop, and the next slide flashed onto the screen.



Principle 3. Generalize Your Opponent's Specific Statements

The Church–Turing thesis proves that no function computable by a finite algorithm can possibly implement a random oracle. FDH RSA is **secure in the Random Oracle Model** [Cor00]. Hence FDH RSA cannot be securely implemented.

He paused for a moment, allowing the words to settle in the room before he spoke again.

*“Here, the tactic is subtle but powerful. You take your **opponent's argument** and **Interpret** it in a **radically different way** - twisting its meaning to suit your own narrative. Once you've reshaped it, you then proceed to **refute this distorted version as though it were the original point being made**. It's a classic strategy, one that can derail a debate before your opponent even realizes what has happened”.*

*“Consider this”, Schopenhauer continued, his voice taking on a more serious tone. “An argument might accurately describe something as a **true random oracle**, but by deliberately omitting the word **true**, you open the door to ambiguity. Without that key term, the concept becomes less grounded, more malleable. And when you refute the vague version—the one without the qualifier - you're attacking a ghost of the original argument, a distorted phantom that cannot stand up to logical scrutiny”.*

“Let's move to the next slide”:



Principle 4. Conceal Your Game

Any cipher encrypting **only half of its plaintext** is insecure. Let t be a binary string and denote by $||t||$ the Hamming weight of t . Let x, y be two n -bit strings and denote $f(x, y) = x \oplus y$. Assume the existence of a perfect randomness source allowing to sample random binary strings. $y \in_R \{0, 1\}^n \Rightarrow ||f(x, y) \wedge x|| \simeq n/2$. In other words, after the xor $\simeq 50\%$ of x 's bits will remain invariant. $f(k, m)$ is an encryption function invented in 1882 by Frank Miller [Bel11, Mil82] where, *mutatis mutandis* instead of using addition modulo 14000, addition modulo 2 is used. Because f encrypts only $\simeq 50\%$ of its bits, i.e. **only half of its plaintext**, f is insecure. f is what the adverse party calls a **“one-time-pad”**.

“This, my friends, is the essence of the long game in debate. You must conceal your ultimate objective until the precise moment when it can no longer be avoided. If you reveal your end goal too soon, your opponent will recognize the trap and reject the path you want them to take. But if you let them reach the milestones gradually, they will unwittingly agree to positions they would have vehemently denied if they had understood your final destination”.

He gave a small, almost imperceptible smile, then continued.

*“Consider the **pivotal argument** - a key point that will determine the outcome of the debate. But notice how it is introduced. Only half of the argument is presented early on, a piece of the puzzle that seems trivial or inconsequential in the moment. It is only later - at the precise moment when you have led your opponent down the desired path - that the*

other half is revealed, completing the argument and making the entire structure of your reasoning appear inevitable. Note how the ‘only half of its plaintext’ was sown at early to be harvested at the end”.

“This,” Schopenhauer said, “is the art of misdirection in debate. You must never reveal your final objective too early. Keep it hidden, concealed in the shadows, so that your opponent cannot anticipate the path you are leading them down. They will agree to small, seemingly harmless steps—milestones along the journey—that they would have flatly rejected, *had they known the end* to which those steps would lead. Consider this:”

We use the third case of Theorem 2, apply an *obvious transformation* to the simulator from Lemma 7 and make two copies of the adversary in Theorem 3. All combined, it follows that the protocol (full paper version) is *computationally zero-knowledge*.

“We craft a convoluted argument that obscures the logical path, presenting results in a seemingly-random order to confuse the reader and introducing subtle modifications. Furthermore, results are not invoked as such but with ‘subtle’ modifications (third case of Theorem 2, modifications to Lemma 7, copies of Theorem 3...). Simultaneously, part of the argument is claimed to be *obvious* while remaining unspecified, hiding the trail in an attempt to mislead the adverse party.”

A further keystroke displayed:

Principle 5. False Propositions

- RSA is as hard as integer factoring;
- The record for RSA breaking is 829 bits moduli;
- Therefore, factoring RSA moduli larger than 900 bits is hard.

“Derive a logically valid *conclusion* from an *incorrect proposition* as a premise. If the conclusion is true, we may claim it ‘validates’ the incorrect proposition⁵. If false, present the reasoning as a proof. *True statements* can also be used as support. Remember: Using false premises is crucial, as both true and false conclusions can logically follow from them, while true premises can only lead to true conclusions”.

Schopenhauer raised an eyebrow and, with a slight grin, pressed another button on his laptop. “And how about this one?” he asked, his voice tinged with curiosity and a hint of mischief. The slide changed, revealing yet another intricate strategy.

Principle 6. Postulate What Has to Be Proved

- Theorem 4 is *mathematically sound* because it is *scientifically accurate and logically correct*.

⁵ Bon sang ne saurait mentir.

“This technique, also called a circular argument, restates the matter instead of actually proving it, to create the *illusion* of a proof:”

Bart Preneel is a *great speaker* because he *presents very well*.

“The *begging the claim* variant makes the *premises* appear as a *conclusion*:”

The obsessive quest of those *nonexistent* cryptographic multilinear maps is useless.

Schopenhauer’s grin widened as he surveyed the new slide. “And those two are cute as well,”



Principle 7. Yield Admissions Through Questions

We all know that only NTRU can possibly preserve cryptography from quantum computers. Don’t we?

“This old technique, also called *rhetorical questioning* is a figure of speech in the form of a question. It consists in asking a question that does not requires a reply to make a point”.



Principle 11. Generalize Admissions of Specific Cases

[BGJT14] shows that discrete logarithms can be computed in $n^{O(\log n)}$ i.e. in (quasi) polynomial time. This calls for an urgent *phase-out of discrete logarithm cryptosystems*.

“This technique is used when prosecution grants defense the benefit of a *particular circumstance*. Building upon this grant, the defender introduces a *general conclusion* as an admitted fact. Preserve the order of the sentences to simplify understanding: *blue* \implies *red*”.

“In the example, the admission is that some discrete logarithms can be computed in $n^{O(\log n)}$. We nonetheless rush ahead and shamelessly generalize this to all discrete logarithms.” “And, defense would typically be refined to”:

[BGJT14] shows that discrete logarithms can be computed in $n^{O(\log n)}$ i.e. in (quasi) polynomial time. This Eurocrypt’14 best paper award result of Gödel prize winner Joux calls for an urgent phase-out of discrete logarithm cryptosystems.

“And remember, every word matters! In this mix of **11** and **30** the correct reference would have been “Barbulescu et al”. Nonetheless, defense voluntarily puts forward Joux who is a Gödel prize winner to appeal to authority rather than to reason. “result” is left in singular and a comma is omitted between “Joux” and “calls” to give the subliminal impression that Joux (in person) recommends the phase-out. The importance of the combining form “quasi” is diminished using parentheses. Parentheses mark contents as secondary”.

Schopenhauer's fingers danced across the holographic interface with the practiced ease of a pianist approaching a familiar sonata. The audience had grown silent, mesmerized not just by the content, but by the theatrical precision with which this 19th-century philosopher was dissecting 21st-century academic discourse. "Ah, *but we are just getting started*", he said, his voice carrying a note of anticipation that made several audience members shift uncomfortably in their seats. "Let us examine the art of metaphorical manipulation."



12. Choose Metaphors Favorable to Your Proposition

A **cipher** is an **armor** around a communication much like a **safe** is an **armor** around a possession. A person who puts something in a safe to which they have the only key or combination surely has both a subjective and objective reasonable expectation of privacy regarding the contents.

"A *metaphor*", Schopenhauer explained, his eyes gleaming with intellectual pleasure, "is an identification of two items based on an implicit or an explicit property that they have in common called *tertium*. This technique is most efficient when the *phora* is very different from the *thema*. It has a strong visual appeal and a strong emotional potential." He paused, letting his gaze wander across the faces in the audience. Several cryptographers were furiously scribbling notes, while others looked as if they were reconsidering every paper they had ever written. "The beauty of this technique", he continued with a slight smile, "lies in its ability to transport legal precedents from one domain to another. Observe how masterfully this is executed". His finger traced the air as he quoted from memory: "It is possible to use the metaphor technique while explicitly treating the *thema* and *phora* differently. Consider this elegant example from [Fro94]:"

"Simply putting something into a safe does not, however, ensure that it is beyond the law's reach. It is settled law that a criminal defendant can be forced to surrender the physical key to a physical safe, so long as the act of production is not testimonial. Presumably *a similar rule compelling production would apply to a criminal defendant who has written down the combination to a safe on a piece of paper*. There appears to be no authority on whether a criminal defendant can be compelled to disclose the combination to a safe that the defendant has prudently refrained from committing to writing, and in *Fisher v. United States*, the Supreme Court hinted that *compelling the disclosure of documents similar to a safe's combination might raise Fifth Amendment problems*. Perhaps the combination lock problem does not arise because the police are able to get the information from the manufacturer or are simply able to cut into the safe. *These options do not exist when the safe is replaced by the right algorithm*. Although brute-force cryptography is a theoretical possibility, neither safe cracking, nor number crunching, nor an appeal to the manufacturer is a practical option when the armor is an advanced cipher."

"Magnificent!" Schopenhauer exclaimed, his voice rising with genuine admiration. "Here the author uses the metaphor identifying *a safe and an algorithm*, only to later

claim that *what applies to the first may not apply to the second*. The metaphor serves its purpose and is then conveniently abandoned when it becomes inconvenient.” A nervous chuckle rippled through the audience. Anna Kowalska, watching from the side of the stage, noticed that several of the attendees were now looking rather pale. “But wait”, Schopenhauer said, his tone taking on the theatrical flair of a master showman, “there is more artistry to unveil!”



Principle 13. Agree to Reject the Counter-Proposition

We can either *use AIS-20/31 certified random number generators* or *expose products to terrible attacks*.

“This technique, also called the ‘either/or dilemma’ consists in offering the illusion of choice (*red xor blue*), by presenting two alternatives. The *undesirable one* is painted in the dimmest possible light to make the audience agree that it must be rejected.” Schopenhauer’s expression grew mischievous. “The example intentionally ignores the gamut of choices in between—using NIST-certified generators, using provably secure PRNGs, and so forth. It’s the intellectual equivalent of asking someone whether they prefer to be shot or hanged, conveniently ignoring that perhaps they might prefer neither.” The audience was beginning to recognize uncomfortably familiar patterns. “And now”, Schopenhauer continued, his voice dropping to a conspiratorial whisper, “we arrive at one of my personal favorites—the art of the seemingly absurd proposition.”



15. Use Seemingly Absurd Propositions

After two decades of extremely intense cryptanalytic efforts, AES is holding very strong. The battle between the cryptographer and the cryptanalyst was definitely won by the cryptographer. Secret-key cryptography has thus reached its end.

“If you happen to be in difficulty to prove your point, ask the opponent whether they agree to a valid (but irrelevant) claim. If they don’t, point out that they are being unreasonable. If they do, pretend that this claim is actually the proof of your position.” He raised a finger with professorial authority. “Note that we did not use the wording ‘still holding’ which conveys a temporality notion but the word ‘strong’. Every word is a weapon, my friends. Every word.” The audience was now completely silent, hanging on his every word. Some looked fascinated, others horrified, and a few appeared to be having existential crises about their entire academic careers. “But perhaps”, Schopenhauer said with a wicked grin, “you prefer the more... personal approach?”



16. Arguments Ad Hominem

A *long list of unrigorous schemes and the privacy-compromising products in which those schemes are used*, raise *concerns about the scientific independence of Nac-cache’s assessment of [6]*.

*“This technique attempts to dispel **an argument** by attacking the **credibility of its author**. The attack on the author is not the goal but a means to refute his argument.”* Schopenhauer’s tone became almost pedagogical. *“Ad hominem attacks must be carefully dosed because audience would naturally tend to express sympathy towards the attacked and because ad hominem arguments trigger very virulent defensive reactions. Use only **one or two grievances** to avoid giving the impression of an irrational all-out war.”* Several audience members glanced at David Naccache, who was sitting in the third row, seemingly very amused by being used as an example by a character in one of his own novels.

“Of course”, Schopenhauer continued smoothly, “when you find yourself under attack, you must master the art of the elegant escape.”

17. Defense Through Subtle Distinction

[UVW17] describe **an attack** on our cryptosystem that is **merely a weak-key, quasi-polynomial attack**. Furthermore their proof does not go through due to the slightly different model that they used for algebraic groups.

“As the name implies, this strategy consists in escaping by way of a ‘subtle distinction’ that hadn’t occurred to you so far, and casts doubt on the argument.” He leaned forward conspiratorially. *“Use ‘furthermore’ instead of ‘but’! The word ‘but’ voids whatever you said before—it is just taken as a calming pill administered in prevision of the attack following the ‘but’.”* The linguistic precision was beginning to unnerve several attendees. Professor Chen from Singapore whispered to his neighbor, *“I need to rewrite my entire rebuttal letter.”* *“Sometimes”, Schopenhauer said with theatrical timing, “the situation becomes so dire that one must resort to... more dramatic measures.”*

18. Interrupt, Break, Divert the Dispute

This is preposterous, just because you are the ePrint editor and I am not doesn’t mean you are allowed to mock me and my work! I’m going to the Ethics Committee of the IACR right now to report this unacceptable behaviour!

“If you are losing the argument, change the topic.” His delivery was so matter-of-fact that several people in the audience burst out laughing despite themselves. *“But perhaps”,* he continued, his eyes twinkling with amusement, *“you prefer the more sophisticated approach of intellectual expansion?”*

19. Generalize the Matter, Then Argue Against it

[FtE07]: From a systems’ approach, Gratzner and Naccache assume that they completely understand the processor’s instruction set and the computer’s architecture. Our experience doesn’t support this view. Real-world systems are riddled with undocumented instructions, hidden registers, and so on.

“Should your opponent expressly challenge you to produce any objection to his argument, expand the argument to the point that you reach the inevitable fallibility of human knowledge, and give various illustrations of it.” Schopenhauer paused, letting the implications sink in. *“It’s the academic equivalent of responding to a criticism of your dinner by questioning whether we can truly know anything about the nature of taste itself.”* The audience was now fully absorbed in this philosophical deconstruction. Some were taking notes frantically, others were staring into the middle distance with expressions of dawning horror. *“And here”*, Schopenhauer said, his voice taking on the tone of a master craftsman revealing his finest work, *“we have the art of premature conclusion.”*

20. Draw Conclusions Yourself

So at this point we all agree that the GCM mode of operation has a good track record and is patent-free, so **this is our only option, and we will now use it for all projects.**

“Don’t let the opponent phrase your conclusion; as soon as enough premises are accepted, invoke non causae ut causae and draw the conclusions yourself. This is easier in writing (non-interactively) where the reader cannot object.” “Of course”, he added with a sly smile, *“when faced with particularly egregious bad faith, one may be forced to respond in kind.”*

21. Meet Him With a Counter-Argument as Bad as His

[14] expresses doubts about the correctness of Theorem 7. This is totally irrelevant because the validity of our identification scheme relies on Theorem 4 only.

“If the opponent hits low with a fallacious argument, you may reciprocate by using an equally-fallacious argument.” Schopenhauer’s expression grew more serious. *“And finally, we arrive at the ultimate defensive maneuver—the recognition of circular reasoning in others.”*

Begging the Question

22. Proving zero-knowledge is not about the hardness of the problem on which the protocol is based but about demonstrating the simulatability of the protocol.

“If your opponent requires you to admit something from which the point in dispute will immediately follow, you must refuse to do so, declaring that it is a petitio principii.” The philosopher paused, his holographic form shimmering slightly as he surveyed the utterly silent auditorium. The weight of recognition was palpable—every person in that room had either used these techniques or been their victim, often both. *“And there you have it”*, he said softly, his voice carrying the weight of centuries of intellectual combat. *“The tools of persuasion, laid bare. The question that remains is not whether these techniques are effective—they manifestly are—but whether we have the wisdom to recognize them when they are used against us, and the integrity to resist using them ourselves.”*



24. State a False Syllogism

...(1) Clipper was an example of government regulation of cryptography; (2) Clipper would result in reducing people's privacy; therefore (3) government regulation reduces people's privacy, which is a bad thing...

"This delicious example comes from [Swi97]", Schopenhauer noted with appreciation, "where defense develops a seemingly deductive argument to convince that the conclusion is true. Observe the logical structure—it appears sound, yet rests upon a foundation of sand. The syllogism is false because it generalizes from a single, carefully chosen instance to establish a universal principle."

Schopenhauer's expression brightened with what could only be described as intellectual mischief. "And speaking of carefully chosen instances, let us examine this delightful technique."



25. Find One Instance to the Contrary

RSA is riddled by fundamental flaws. Indeed, parameter choices such as $d = 1$, $m = 0$ or $m = 1$ make RSA disastrously insecure.

"This technique refutes a thesis by pointing out at least one exotic instance to which the thesis does not apply", he explained, his voice carrying the tone of a professor who had discovered a particularly fine specimen.

He paused, allowing his gaze to sweep across the room. "I am told that similar approaches sufficed to get papers accepted to SPRC and PKC [Nac93, CN99]. In both cases, simple equality tests would have avoided the attacks entirely... but where would be the drama in that?"

"But perhaps the most elegant technique of all", Schopenhauer continued, his voice taking on an almost conspiratorial tone, "is the art of the perfect reversal."



26. Turn the Tables

[17] considers that since $SIDH^a$ is relatively new, it has not undergone enough scrutiny to be deployed in practical applications. In truth, it is precisely because $SIDH$ is relatively new, that no attacks are known against it and its early adopters will stay one step ahead of hackers.

^a Supersingular Isogeny Diffie-Hellman key exchange (SIDH)

"Reuse your opponent's premises to draw a different or opposite conclusion", Schopenhauer explained with evident satisfaction.

His expression grew more philosophical. "The adverse party will never be convinced, of course. Remember: 'A jury consists of 12 persons chosen to decide who has the best lawyer.'⁶ Good storytelling—a mix of material facts, hypotheses and appealing to emotions—will inevitably make the jury feel as if they were present at the crime scene where things happened exactly as told."

⁶ Robert Frost.

The audience was beginning to realize that they were not merely learning about rhetorical techniques—they were witnessing a master class in intellectual manipulation, delivered by perhaps its greatest historical practitioner.

“*And when all else fails*”, Schopenhauer said, his tone shifting to that of a magician about to reveal his greatest trick, “*there is always the art of misdirection.*”

29. Diversion

To explain our attack on Cramer–Shoup we must first recall the notion of *group*. Note that groups also appear in physics, in particular Lie groups, for example $SO(3)^a$. Its double cover is $SU(2)$, which is canonically represented using complex-valued matrices [plug here a tiring dissertation about groups]. This completes our overview of the 26 exceptional groups (called sporadic groups) found in the classification of finite simple groups. We are now ready to focus on the attack’s efficiency.

^a Which is the group of all rotations about the origin of three-dimensional Euclidean space \mathbb{R}^3 under the operation of composition.

“If you are in a *weak position*, slowly but surely *diverge from the subject* and lure your opponent to follow you *somewhere else*”, he explained, his eyes twinkling with amusement. “Just as misdirection in theatrical magic—a form of deception where the magician draws audience attention to one thing to distract it from another—diversion exploits Parkinson’s law of triviality, according to which audience gives disproportionate attention to trivial items. This relieves focus from the weak position and hence helps defense.”

“But perhaps”, Schopenhauer continued, his voice dropping to an almost reverent whisper, “the most powerful technique of all is the one that requires no original thought whatsoever.”

30. Appeal to Authority Rather Than Reason

Our proof follows the methodology refined in a thread of papers by Rivest [23], Shamir [26] and Goldwasser [7]. Note that the same approach was adopted by Micali in [11,12,13], Yung in [31,33], Gentry in [4,5,6] and Pointcheval in his two seminal papers [14,16].

“In the following, authorities are quoted twice”, Schopenhauer observed with the clinical precision of a surgeon. “The *first list* suggests truthfulness whilst the *second* attempts to convince the reader that adopting the technique is jurisprudence. The plurality of references per author hints at routine use.”

He paused, letting the implications sink in. “Why burden yourself with the exhausting work of original reasoning when you can simply invoke the names of those who have reasoned before you? It is intellectual outsourcing at its finest.”

Schopenhauer’s holographic form seemed to grow more animated as he progressed through his arsenal of rhetorical weapons.

“Now”, he said, his voice taking on the tone of a master craftsman revealing his most prized tools, “*we arrive at the art of false modesty—perhaps the most insidious weapon in the academic arsenal.*”



31. This is Beyond Me

Being a number-theorist, symmetric cryptography is really not my area. This makes the flaws pointed-out in the previous paragraph obvious. Reject.

“Exploit the speaker’s real or purported ignorance as an obviousness argument to hint Occam’s razor⁷: If an ignorant understands the argument then it must be direct and truthful.”

Schopenhauer’s eyes gleamed with particular satisfaction. *“Using this strategy calls for careful plea engineering. The pleader must be ignorant enough—a young counsel, perhaps—because a reputed expert can hardly portray himself as ignorant. A reputed counsel would usually mention that he is a specialist of a different field and hence legitimately ignorant in the subject matter.”*

He raised a finger with professorial authority. *“But beware! If the speaker portrays himself as too ignorant, the audience may be tempted to also try and follow the reasoning—and hence discover the fallacy. The pleader would therefore use sentences such as ‘Even for a specialist of marine law such as myself this income tax question is clear as the conclusion stems from general, law school-level, constitutional law principles’. Because the audience is likely not to know constitutional law in detail, they deter themselves from attempting to follow the argument.”*

A knowing smile crossed his features. *“And remember—use ‘clear’ rather than ‘evident’ or ‘trivial’. The linguistic precision is everything.”*

Several audience members shifted uncomfortably, recognizing this exact pattern from recent conference reviews. Dr. Hartmann whispered to her colleague, *“That’s exactly what Reviewer 2 said about my lattice paper.”*

“But when subtlety fails”, Schopenhauer continued, his voice dropping to a more ominous tone, *“one may be forced to deploy the nuclear option—guilt by association.”*



32. Put His Thesis into Some Odious Category

The Internet Watch Foundation reports^a that nearly all pedophile websites accept cryptocurrency in exchange of their disgusting contents. While human cloning research is stained with blood, cryptocurrency research is stained with children’s blood. This “research” is nothing but the fabrication of torture instruments tantamount to the sadistic “research” performed on helpless children by Mengele in Auschwitz. Any person right in his mind, must deny any ethical and scientific credit to “papers” published in the ACM Workshops on Blockchains,

⁷ *entia non sunt multiplicanda praeter necessitatem*

Cryptocurrencies and Contracts and, in particular to the “results” clamied in [12].

^a <https://www.iwf.org.uk/what-we-do/who-we-are/annual-reports>

A visible shudder ran through the audience. Schopenhauer’s expression grew grave. “This technique, also called *Reductio ad Hitlerum*, belongs to the category of pathos arguments⁸. It is meant to appeal to the jury’s values and emotional sensibilities. It attempts to dismiss the adverse position on the basis that the same view was held by an odious person.”

He gestured with the air of a warning. “For example:”

Cryptographers who accept the Marconi Prize are the first fascists in their field as they perpetrate the memory of Marconi, a member of the Grand Council of Fascism who said “I reclaim the honor of being the first fascist in the field of radiotelegraphy”

“This belongs to the class of arguments to the consequence⁹: conclude a belief as either true or false based on whether the premise leads to desirable or undesirable consequences.”

33. It Applies in Theory, but Not in Practice

Whilst computing an RSA signature is – *in theory* – polynomial, constant advances in factorization make keys increasingly longer. Unfortunately, signing time is proportional to the cube of the key size. As a result, RSA is already unfit as a realistic digital signature option.

“Note the words “*in theory*”, subtly emphasized in the sentence”, Schopenhauer observed with clinical precision. “This should not be confused with bona fide theory versus practice arguments such as [CGH04]¹⁰. The beauty lies in the dismissive implication that theory is somehow lesser than practice—a remarkable position for an academic field to take.”

“But sometimes”, Schopenhauer said, his voice taking on an almost conspiratorial whisper, “the most effective argument is the one that attacks your opponent’s very livelihood.”

⁸ emotional appeal

⁹ *argumentum ad consequentiam*

¹⁰ Here insecurity is theoretical but not necessarily practical. “The main result of this article is a negative one: There exist signature and encryption schemes that are secure in the Random Oracle Model, but for which any implementation of the random oracle results in insecure schemes. In the process of devising the above schemes, we consider possible definitions for the notion of a ‘good implementation’ of a random oracle, pointing out limitations and challenges.”



35. Will Is More Effective Than Insight

Surely one cannot seriously claim that $P = NP$, otherwise cryptography is dead and we're all out of a job!

“Show that your opponent’s arguments, when pushed to their fullest conclusion, impact your opponent negatively”, he explained with evident satisfaction. “It is the intellectual equivalent of threatening to burn down the village to save it. Remarkably effective, particularly in academic circles where career preservation often trumps intellectual honesty.”

A nervous laugh rippled through the audience, though it was unclear whether they were laughing at the technique or recognizing its uncomfortable familiarity.

“And finally”, Schopenhauer announced, his voice rising with theatrical grandeur, “we arrive at the technique that has launched a thousand dissertations and sunk a thousand more—the art of intellectual intimidation.”



36. Bewilder Your Opponent by Mere Bombast

Assuming the Riemann hypothesis and $P \neq NP$, the proof relies upon the classical notions of computational indistinguishability, the Baker–Gill–Solovay theorem, probabilistic polynomial-time observers, the generic group model and invertible measure-preserving transforms.

“The sentence attempts to undermine the reader’s self-confidence using an intimidating exordium and an intimidating peroration”, Schopenhauer explained, his voice carrying the satisfaction of a master who had identified the perfect specimen. “The technique is as simple as it is effective: pile on so many impressive-sounding concepts that the reader assumes their inability to follow the argument must be due to their own intellectual inadequacy rather than the author’s deliberate obfuscation.”



37. A Faulty Proof Refutes His Whole Position

OAEP is widely believed to provide resistance against adaptive chosen ciphertext attack. The main justification for this belief is a supposed proof of security in the random oracle model, assuming the underlying trapdoor permutation scheme is one way. This paper shows conclusively that this justification is invalid. First, it observes that there appears to be a non-trivial gap in the OAEP security proof. Second, it proves that this gap cannot be filled, in the sense that there can be no standard “black box” security reduction for OAEP. This is done by proving that there exists an oracle relative to which the general OAEP scheme is insecure. [...]. It should be stressed that these results do not imply that a particular instantiation of OAEP, such as RSA-OAEP, is insecure. They simply undermine the original justification for its security. In fact, it turns out—essentially by accident, rather than by design—that RSA-OAEP is secure in the random oracle model; however, this fact relies on special algebraic properties of the RSA function, and not on the security of the general OAEP scheme.

*“Leverage **one mistake** in your opponent’s proof to deploy an argumentum ad rem (as in the above quote from [Sho02]) or an attack ad hominem”, Schopenhauer explained, his holographic form seeming to shimmer with particular satisfaction. “This technique exploits the academic tendency toward perfectionism. Find a single flaw—no matter how minor or correctable—and use it to cast doubt upon the entirety of your opponent’s work.”*

He gestured toward the example with theatrical precision. *“Observe the masterful construction: the authors acknowledge that their critique does not invalidate the practical security of RSA-OAEP, yet they frame their argument as showing the justification is ‘conclusively invalid’. The psychological impact is devastating—readers remember the strong condemnation far more than the careful technical limitations.”*

His voice took on an almost conspiratorial whisper. *“The beauty lies in the asymmetry of effort. Your opponent may have spent years constructing a complex proof with ninety-nine correct steps, but you need only find one questionable transition to declare the entire edifice unsound. It is intellectual warfare at its most efficient.”*



38. Become Personal, Insulting, Rude

... Alfredo DeSantis (University of Palermo) spoke on “Graph decompositions and secret sharing schemes”, a silly topic that brings joy to combinatorialists and yawns to everyone else [...] Yvo Desmedt, the “mad Belgian”, seems to have caught on at the University of Wisconsin, Milwaukee. He’s also been getting respect from the IACR, being on the Program Committee and also on the Board of Directors. As befits a person of honor, he no longer rattles the rafters with his staccato delivery [...] But have no sympathy for the much-maligned Professor Schnorr (University of Frankfurt)! In an oft-replayed scenario he was the next speaker and presented “FFT-Hash II: efficient cryptographic hashing”, a small revision of his sullied scheme. [...] An East German, Ralph Wernsdorf (SIT Gesellschaft für Systeme der Informationstechnik mbH; Grünheide) Mark King said that had been told by his German friends that this company was composed of ex-Stasi people) [...] I had all but forgotten about Hellman; he has not been active on cryptologic scene in many years, and I’ve always had doubts about his moral principles (by contrast, I regard Rivest as being above all this dirt). [...] Jim Bidzos, the aggressive RSA representative was unable to attend but curmudgeon Whit Diffie presented a frail RSA position (Bidzos would have much more implacable) and was essentially ignored by the panel...

“This is quoted from [ubcbegftloa94]”, Schopenhauer noted, his expression growing darker. “Distinguish this technique (argumentum ad personam) from technique 16 (argumentum ad hominem). Here we pass from the subject of dispute to the disputant himself and target his person. By opposition, technique 16 passes from the subject of dispute to the disputant to cast doubt on his arguments.”

The philosopher’s holographic form seemed to flicker with disapproval. *“This represents the complete abandonment of intellectual discourse in favor of character assassination. When logic fails, when evidence proves insufficient, when even the most sophisticated rhetorical manipulation cannot carry the day—then, and only then, does one resort to this most base of strategies.”*

He paused, his gaze sweeping across the now thoroughly uncomfortable audience. *“Observe the systematic nature of the assault: ‘silly topic’, ‘mad Belgian’, ‘much-maligned’, ‘sullied scheme’, ‘doubts about his moral principles’, ‘curmudgeon’. Each epithet is carefully chosen to diminish not the work, but the worth of the individual researcher.”*

Schopenhauer’s voice took on a tone of grave warning. *“Yet beware—this technique is a double-edged sword. While it may provide momentary satisfaction and perhaps even tactical advantage, it inevitably reflects more poorly upon the attacker than the attacked. The audience, witnessing such naked hostility, begins to question not the target’s competence, but the attacker’s character. It is the rhetorical equivalent of a suicide bombing—devastating, but ultimately self-destructive.”*

The auditorium had fallen into complete silence. Even the most hardened academics in the audience seemed shaken by this final revelation of their field’s darkest practices laid bare. The weight of recognition was overwhelming—every person in that room had either wielded these weapons or been cut down by them, often in the same paper.

Schopenhauer stood motionless for a long moment, his holographic form shimmering slightly in the stage lights. When he finally spoke again, his voice carried a different quality—less theatrical, more philosophical, almost melancholic.

“And there you have it, ladies and gentlemen. The main arsenal of intellectual warfare, laid bare before you. These are the tools with which we shape not just arguments, but entire fields of human knowledge. The question that remains is not whether these techniques work—they manifestly do—but what kind of scholars, what kind of people, we become when we wield them.”

He paused, his gaze sweeping across the sea of faces before him.

“I have spent my existence—both corporeal and holographic—studying the nature of human will, the drives that compel us to fight, to win, to dominate. And yet, standing here before you, I am struck by a profound irony. You have created machines that can simulate my voice, my appearance, even my thoughts. But the one thing your technology cannot simulate is wisdom—the wisdom to know when victory is not worth the cost of achieving it.”

The audience sat transfixed, hanging on every word of this unexpected philosophical turn.

“You see, the techniques I have demonstrated today are not mere academic curiosities. They are the very mechanisms by which truth is distorted, progress is impeded, and genuine discovery is subordinated to the will to power. Every fraudulent proof that passes peer review, every flawed cryptosystem that is deployed because its proponents were more persuasive than its critics, every young researcher who abandons a promising line of inquiry because they cannot match the rhetorical sophistication of their opponents—all of these are the fruits of the art I have taught you today.”

Anna Kowalska, watching from the wings, felt a chill run down her spine. This was not the entertaining philosophical diversion she had envisioned.

“The tragedy”, Schopenhauer continued, his voice growing more intense, “is that you do not need these weapons. Your field—the study of secrets, of hidden knowledge, of the very foundations of secure communication—this is among the most noble pursuits of human intellect. You are the guardians of privacy, the architects of trust, the defenders

of digital civilization itself. Why, then, some here resort to the tactics of sophists and charlatans?”

The question hung in the air like an accusation.

“Perhaps”, he said after a long pause, “it is because the stakes have grown so high. Perhaps it is because the pressure to publish, to obtain funding, to achieve tenure, has corrupted the very enterprise of discovery. Or perhaps it is simply because these techniques work, and in a world where perception often matters more than reality, the temptation to use them is simply too great to resist.”

Dr. Hartmann found herself wiping away tears, though she couldn’t quite explain why.

“But I ask you to consider this: What if, instead of perfecting the art of being right, you dedicated yourselves to the art of being truthful? What if, instead of learning to win arguments, you learned to conduct them in such a way that truth—rather than victory—was the inevitable outcome?”

The holographic philosopher’s form seemed to grow more translucent, as if the weight of his own words was causing him to fade.

“The choice, as always, is yours. You can use what I have taught you today to become more effective advocates for your own positions, more skillful manipulators of academic or business discourse. Or you can use this knowledge as a mirror, to recognize these techniques when they are used against you, and to commit yourselves to a higher standard of intellectual honesty.”

His voice grew softer, more distant.

“Remember this: The art of being right is easy to master. The art of being truthful—that is the work of a lifetime. And it is work that your field, your civilization, desperately needs you to undertake.”

“Before I conclude,” Schopenhauer said, his voice taking on a warmer tone than it had carried throughout the evening, “I must say that I am particularly pleased to have been called to speak here in Gdansk, my birthplace, on this special occasion”.

He gestured toward the audience with an almost paternal smile. “For I understand that tonight we are not only gathered for Eurocrypt 2030, but also to celebrate the retirement since 5 years of one of your most distinguished colleagues - Peter Ryan”.

In the third row, a distinguish British gentleman with silver hair and kind eyes looked up in surprise. Peter Ryan, now working for British intelligence – following the example of his late father, had been quietly enjoying the philosophical spectacle, never expecting to be mentioned by name. His weathered hands, which had spent decades crafting elegant e-voting schemes, now trembled slightly as all eyes in the auditorium turned toward him.

“Peter,” Schopenhauer continued, his holographic form seeming to look directly at the veteran cryptographer, “though I am but a resurrection of thoughts and words from centuries past, I have been told of your contributions to this field. Your work on verifiable elections, your dedication to the principles of privacy and security - these are not mere technical achievements, but philosophical victories in the eternal struggle between truth and deception, between transparency and concealment”.

The auditorium erupted in spontaneous applause. Peter’s colleagues rose to their feet, acknowledging decades of groundbreaking research and mentorship. But Peter

himself remained seated, overwhelmed by the unexpected honor of being recognized by this most unusual keynote speaker.

“You see,” Schopenhauer observed as the applause died down, “while I have spent this evening teaching you the art of winning arguments through rhetoric and persuasion, Peter Ryan has dedicated his career to the opposite pursuit - ensuring that truth cannot be manipulated, that votes cannot be falsified, that the very foundations of democratic discourse remain secure. In this, he is a far greater philosopher than I ever was”.

A single tear rolled down Peter’s cheek as he absorbed these words. After a lifetime of complex mathematics and rigorous proofs, to be honored not just as a cryptographer but as a guardian of truth itself - and by Arthur Schopenhauer, no less - was beyond anything he could have imagined when he began his career decades ago.

“So let this be my final word,” Schopenhauer concluded, his voice resonating through the now-silent auditorium. “While the art of being right may help you win debates, the pursuit of being truthful - as exemplified by scholars like Peter - is what advances human knowledge. May you all choose wisely between these two paths”.

With that, the holographic figure began to fade, his form becoming translucent as the Holobox powered down. The last thing visible was Schopenhauer’s enigmatic smile, as if he was pleased to have delivered one final paradox - using his own rhetorical skills to argue against the very art he had mastered.

The auditorium remained in respectful silence for several moments after the philosopher had completely vanished. Then, as if by unspoken agreement, the entire assembly rose in a standing ovation - not just for the remarkable technological achievement they had witnessed, but for Peter Ryan, whose life’s work had just been celebrated by one of history’s most formidable intellects.

Anna Kowalska stepped forward to the microphone, her eyes bright with tears of her own. *“Ladies and gentlemen, I believe Arthur Schopenhauer has given us the perfect conclusion to what has been a truly extraordinary evening. Please join me in one final celebration of Peter Ryan’s remarkable career”.*

As the crowd burst into renewed applause, Peter finally stood, raising a trembling hand in acknowledgment. In that moment, surrounded by colleagues and honored by history itself, he felt the profound satisfaction of a life dedicated to truth - a fitting end to both an extraordinary keynote and an extraordinary career.

10.1 An Exercise

In 2007 the author replied in IEEE Security and Privacy Magazine to a critical letter by Dinolt & Garfinkel [FtE07].

Can you identify in the letter and/or in the reply some of the pleading techniques described here?



11 Acknowledgment

The author thanks Rémi Géraud-Stewart for his very insightful suggestions on our tales as well as Ofer Yifrach-Stav for trying to answer as many riddles as possible.

References

- Bel11. Steven M. Bellovin. Frank miller: Inventor of the one-time pad. Cryptologia, 35(3):203–222, 2011.
- BGJT14. Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In Phong Q. Nguyen and Elisabeth Oswald, editors, Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings, volume 8441 of Lecture Notes in Computer Science, pages 1–16. Springer, 2014.
- CGH04. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. J. ACM, 51(4):557–594, 2004.
- CN99. Jean-Sébastien Coron and David Naccache. On the security of RSA screening. In Hideki Imai and Yuliang Zheng, editors, Public Key Cryptography, Second International Workshop on Practice and Theory in Public Key Cryptography, PKC '99, Kamakura, Japan, March 1-3, 1999, Proceedings, volume 1560 of Lecture Notes in Computer Science, pages 197–203. Springer, 1999.
- Cor00. Jean-Sébastien Coron. On the exact security of full domain hash. In Mihir Bellare, editor, Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, volume 1880 of Lecture Notes in Computer Science, pages 229–235. Springer, 2000.
- Fro94. A Michael Froomkin. Metaphor is the key: Cryptography, the clipper chip, and the constitution. U. Pa. L. Rev., 143:709, 1994.
- FtE07. Letters From the Editors, June 2007.
- Mil82. F. Miller. Telegraphic code to insure privacy and secrecy in the transmission of telegrams. C. M. Cornwell, 1882.

- Nac93. David Naccache. Unless modified fiat-shamir is insecure. Proceedings of the third symposium on state and progress of research in cryptography: SPRC'93, pages 172--180, 1993.
- Sho02. Victor Shoup. OAEP reconsidered. J. Cryptology, 15(4):223–249, 2002.
- Swi97. Peter P. Swire. The uses and limits of financial cryptography: A law professor's perspective. In Rafael Hirschfeld, editor, Financial Cryptography, First International Conference, FC '97, Anguilla, British West Indies, February 24-28, 1997, Proceedings, volume 1318 of Lecture Notes in Computer Science, pages 239–258. Springer, 1997.
- ubcbegftloa94. Author unknown but can be easily guessed from the list of attendees. Eurocrypt'92. CRYPTOLOG, XX(1):12–19, 1994. <https://tinyurl.com/NSA94>.