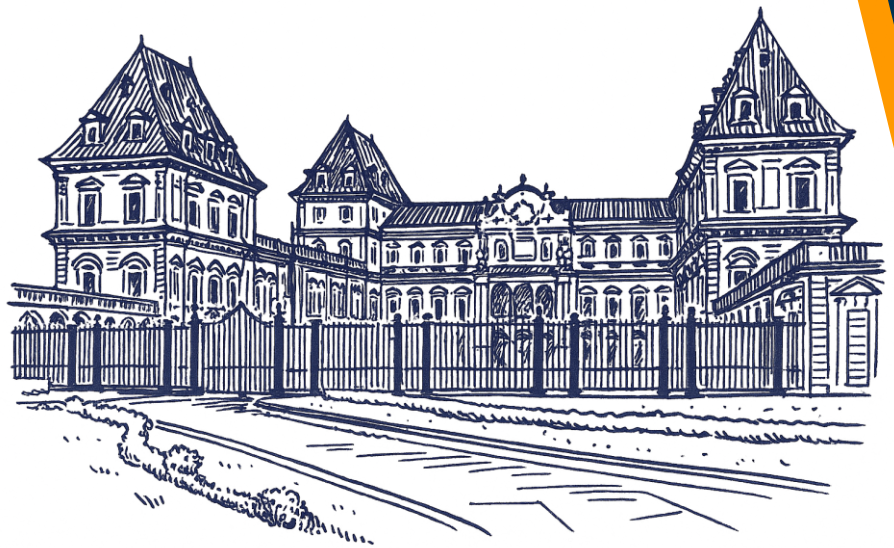


An aperitif on modern cryptography

Leonardo Errati

April 10th, 2026

Politecnico di Torino | CrypTO

INTERLUDE: What Cryptography is Not

Cryptography?

NOT cryptography

AF104CE57016B84840AC04
1E383AC472105A50E0095E
50467ACD0BD49415076A02
9828A623D4932111424084
8BB5190A46630D8463055 7
42898C771AC907892E40E7
965A4DFF46004C89BD7217
6859DB223061A141C274FE
AC1070056339 1DEB92CE06
019507FB59C34AE145589A

cryptography

Cryptography?

Cryptography	Making ciphers
Cryptanalysis	Breaking ciphers
Cryptology	Making & breaking ciphers

1. Against entropy...

Atbash cipher

*“And after all of them, the king of **Sheshak** will drink it too.”*

(Book of Jeremiah, 25:26)

*“Behold, I will raise up against Babylon, and against the inhabitants of **Lev-kamai**, a destroying wind.”*

(Book of Jeremiah, 51:1)

Atbash cipher

*“And after all of them, the king of **Sheshak** will drink it too.”*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf

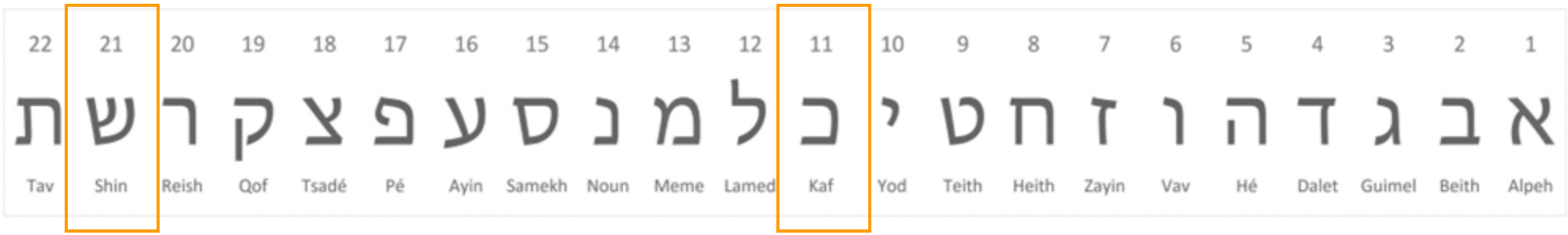
Atbash cipher

*"And after all of them, the king of **Sheshak** will drink it too."*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf $\xrightarrow{\varphi_{atbash}}$ *bet-bet-lamed*



$$\varphi_{atbash}\colon \mathbb{Z}_{22} \to \mathbb{Z}_{22}$$
$$x \mapsto (23 - x)\ mod\ 22$$

A ⟶ Z
B ⟶ Y
C ⟶ X

Atbash cipher

*"And after all of them, the king of **Sheshak** will drink it too."*

(Book of Jeremiah, 25:26)

Sheshak

shin-shin-kaf

φ_{atbash}

Babylon

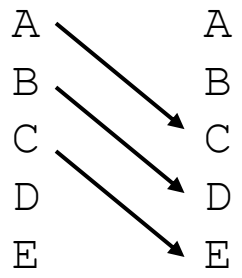
bet-bet-lamed

$$\varphi_{atbash}\colon \mathbb{Z}_{22} \to \mathbb{Z}_{22}$$
$$x \mapsto (23 - x)\ mod\ 22$$

A ⟶ Z
B ⟶ Y
C ⟶ X

Caesar cipher

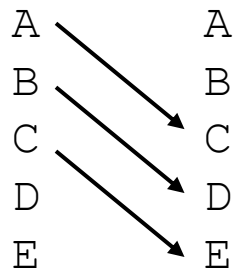

```
message:      ATTACKATDAWN
key:          C
ciphertext:   DWWDFNDWGDZQ
```



Caesar cipher

$$\varphi_{caesar}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x + k)\ mod\ 26$$

```
message:      ATTACKATDAWN
key:          C
ciphertext:   DWWDFNDWGDZQ
```



Caesar cipher

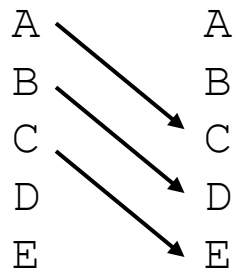
$$H(K) = -\sum_{k \in K} P[k] \cdot \log_2 P[k]$$

$$H_{caesar} \simeq 4.7$$

$$\varphi_{caesar}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$x \mapsto (x + k)\ mod\ 26$$

```
message:      ATTACKATDAWN
key:          C
ciphertext:   DWWDFNDWGDZQ
```



Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$H_{vigenere} \simeq 4.7 \cdot t$$

$$\varphi_{vigenere}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x_i + k_{i \bmod t}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext:   KXRKGIKXBKAL
```

Vigenere cipher

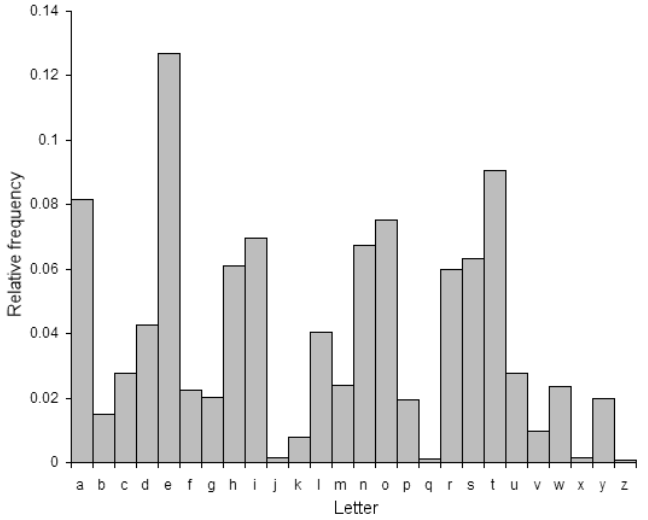
$$k = (k_0, \dots, k_{t-1})$$

$$H_{vigenere} \simeq 4.7 \cdot t$$

statistical attacks

$$\varphi_{vigenere}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x_i + k_{i \bmod t}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext:   KXRKGIKXBKAL
```



Vigenere cipher

$$k = (k_0, \dots, k_{t-1})$$

$$H_{vigenere} \simeq 4.7 \cdot t$$

statistical attacks

key reuse, simple keys

$$\varphi_{vigenere}: \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$x \mapsto (x_i + k_{i \bmod t}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext:   KXRKGIKXBKAL
```

```
COMPLETE VICTORY
MANCHESTER BLUFF
COME RETRIBUTION
```

Vigenere cipher

$$k = (k_0, \ldots, k_{t-1})$$

$$H_{vigenere} \simeq 4.7 \cdot t$$

statistical attacks

key reuse, simple keys

complex

```
message:      ATTACKATDAWN
key:          keykeykeykey
ciphertext :  KXRKGIKXBKAL
```

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vernam cipher

$$k = (k_0, \dots, k_{n-1})$$

$$H_{vernam} \simeq 4.7 \cdot n$$

$$\varphi_{vernam}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$x_i \mapsto (x_i + k_{i \bmod n}) \; mod \; 26$$

```
message:      ATTACKATDAWN
key:          aezklwgrmali
ciphertext:   AXSKNGGKPOHV
```

Vernam cipher

$$k = (k_0, \dots, k_{n-1})$$

$$H_{vernam} \simeq 4.7 \cdot n$$

$$\varphi_{vernam}\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$

$$x_i \mapsto (x_i + k_{i \bmod n}) \bmod 26$$

```
message:      ATTACKATDAWN
key:          aezklwgrmali
ciphertext:   AXSKNGGKPOHV
```

If k is uniformly distributed and independent on m this cipher is perfect, i.e.

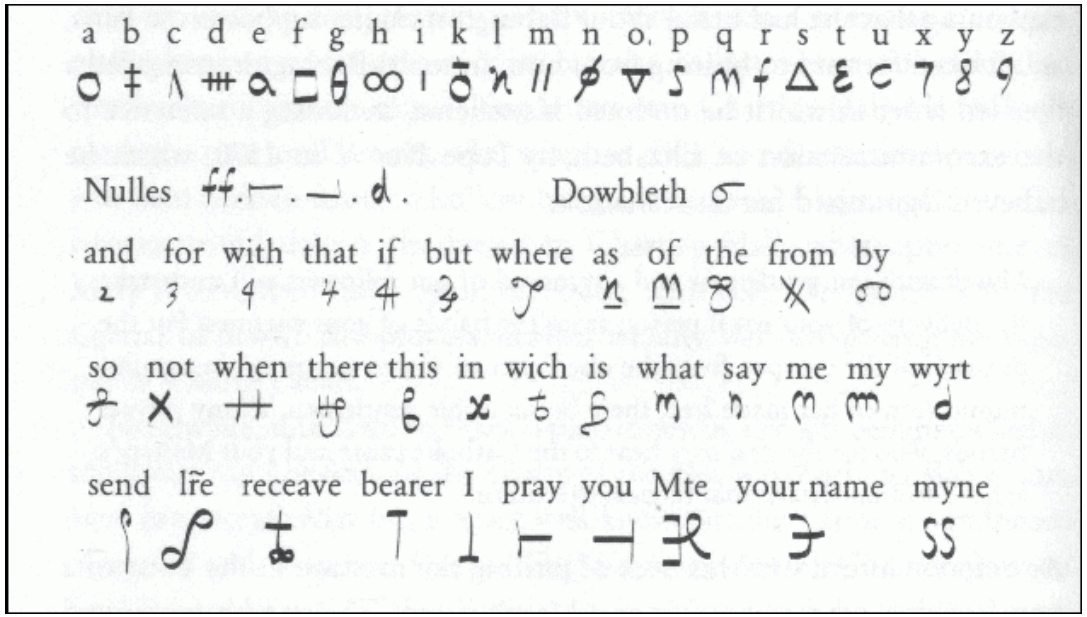
$$P[M = m \,|C = c] = P[M = m]$$

Vernam cipher

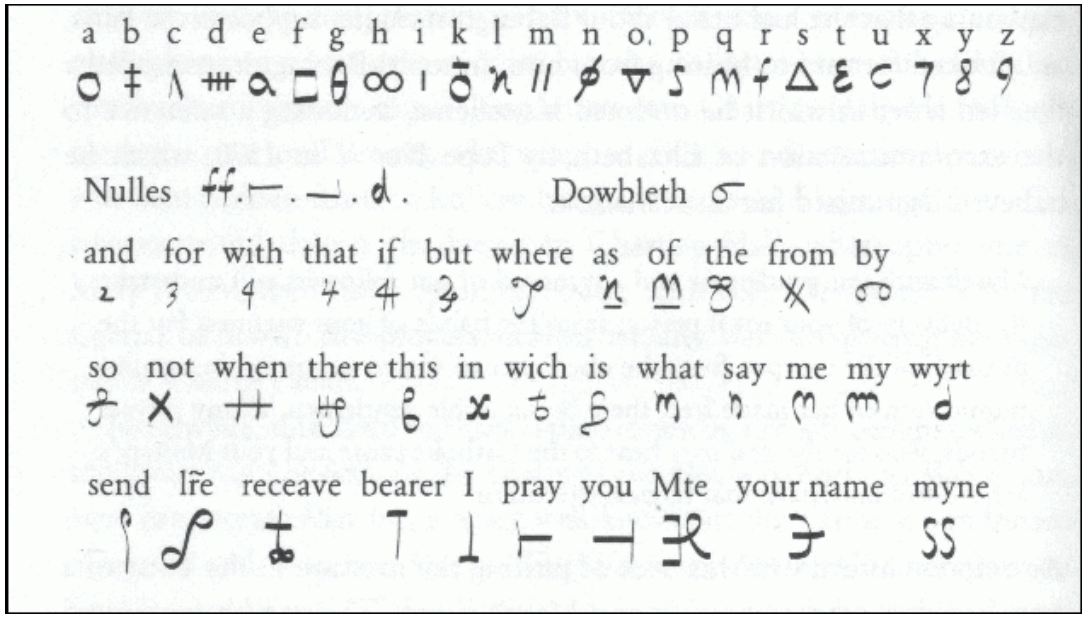

```
message:      ATTACKATDAWN
key:          aezklwgrmali
ciphertext :  KXRKGIKXBYAL
```

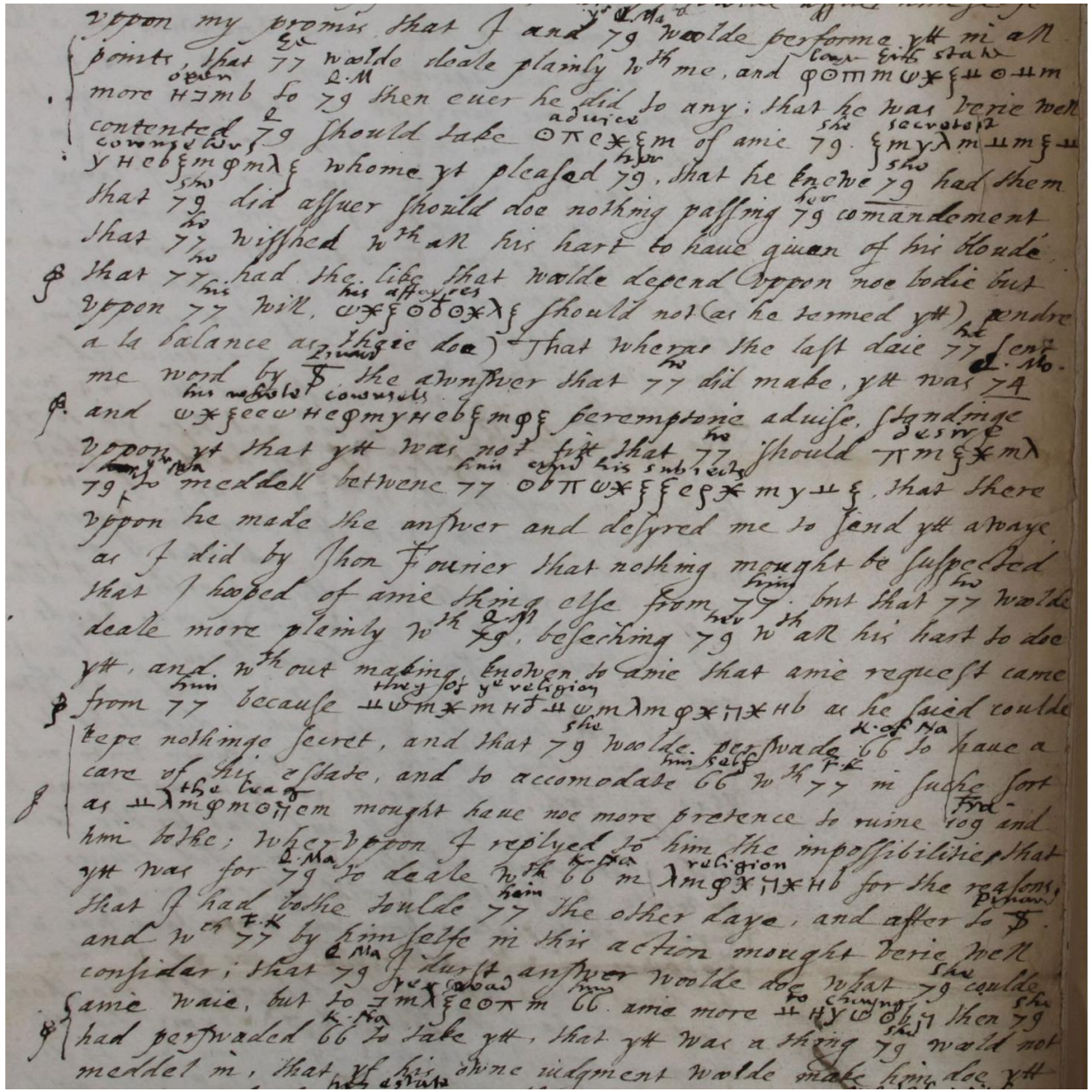
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	**X**	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	S
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Nomenclators

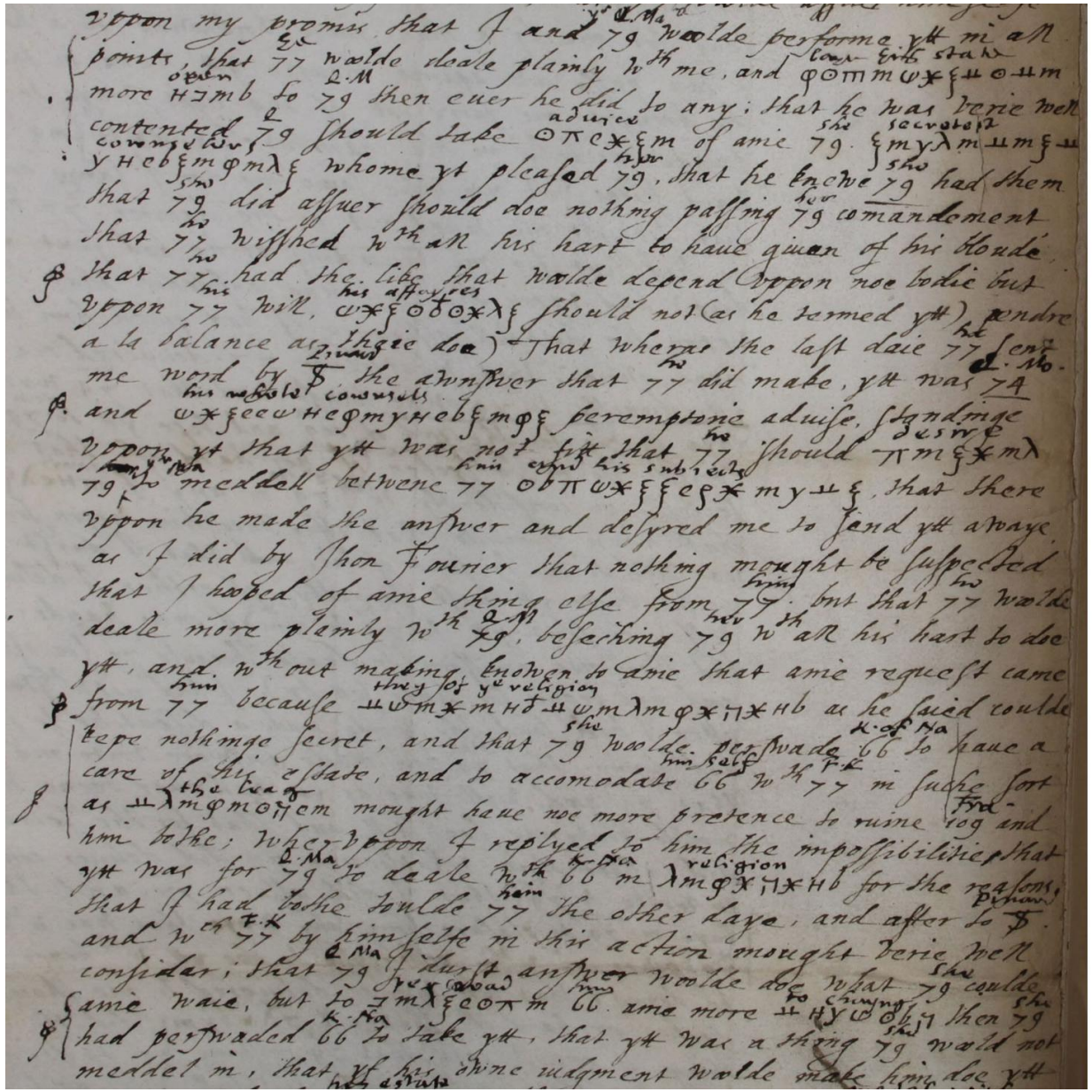


Nomenclators





Nomenclators



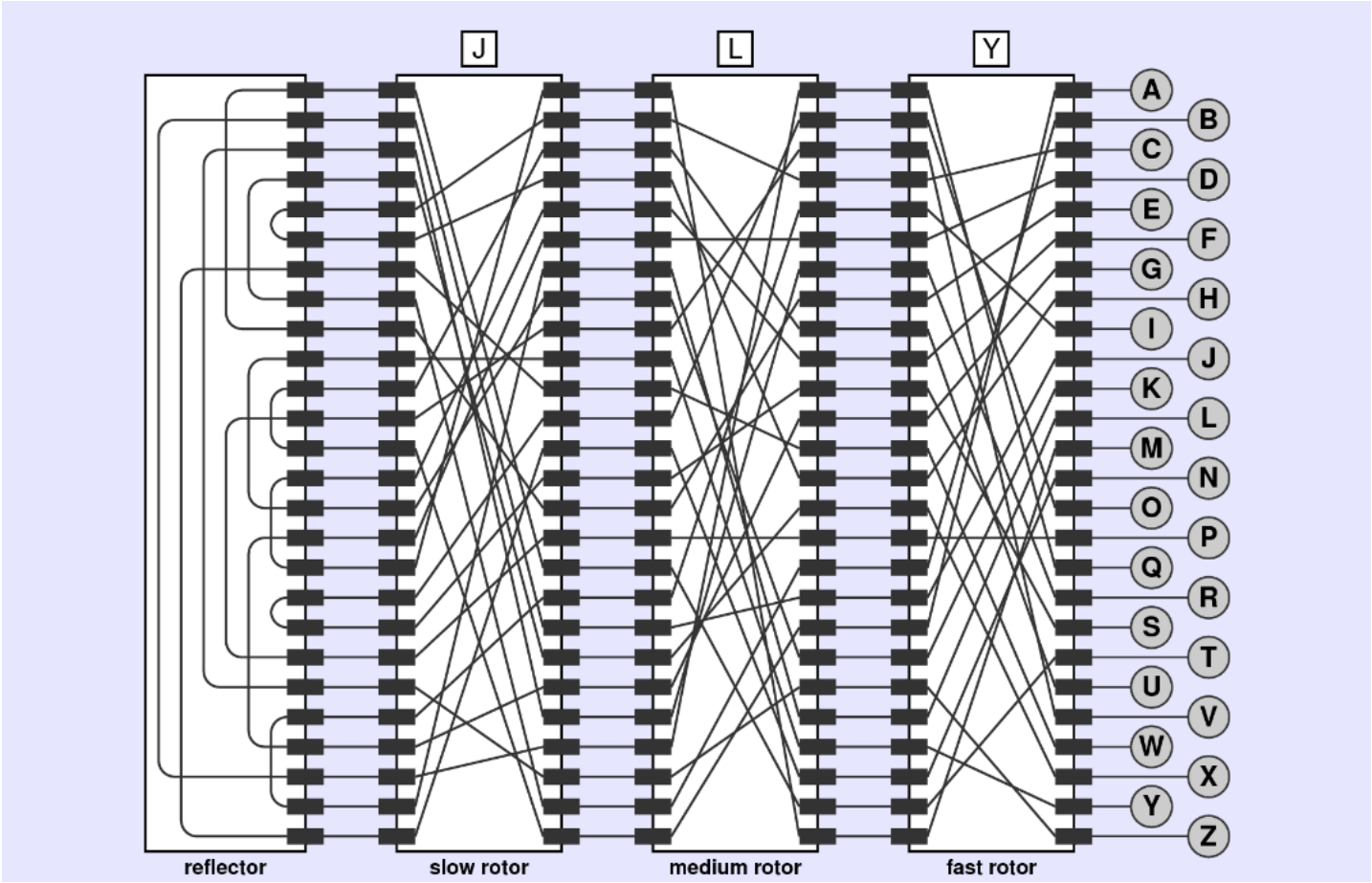
Nomenclators

Take aways

- Bad cryptography causes headaches/beheadings
- Short keys break
- Humans hate complex ciphers

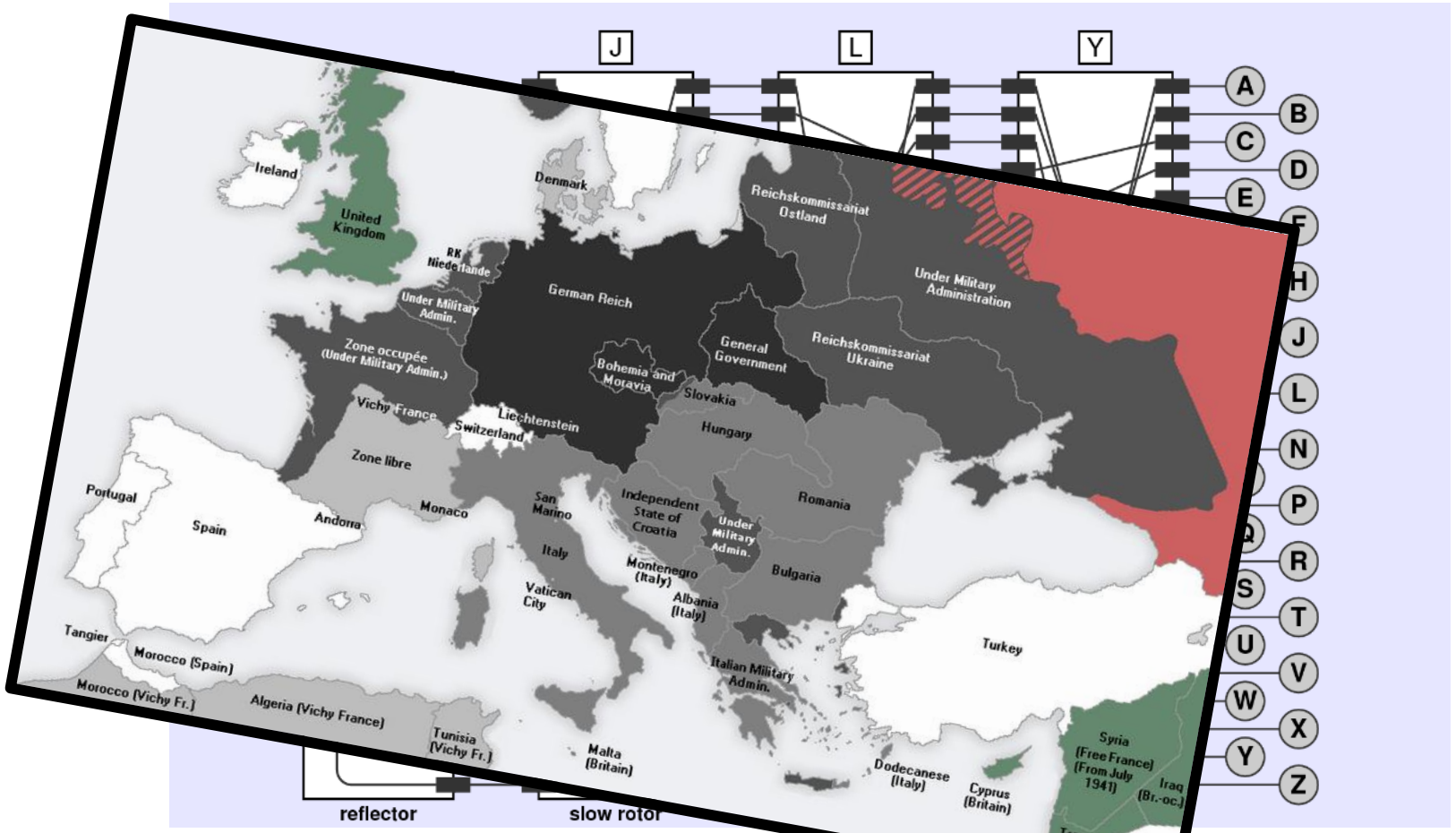
1. Against entropy...
2. Machines themselves...

Enigma cipher machine



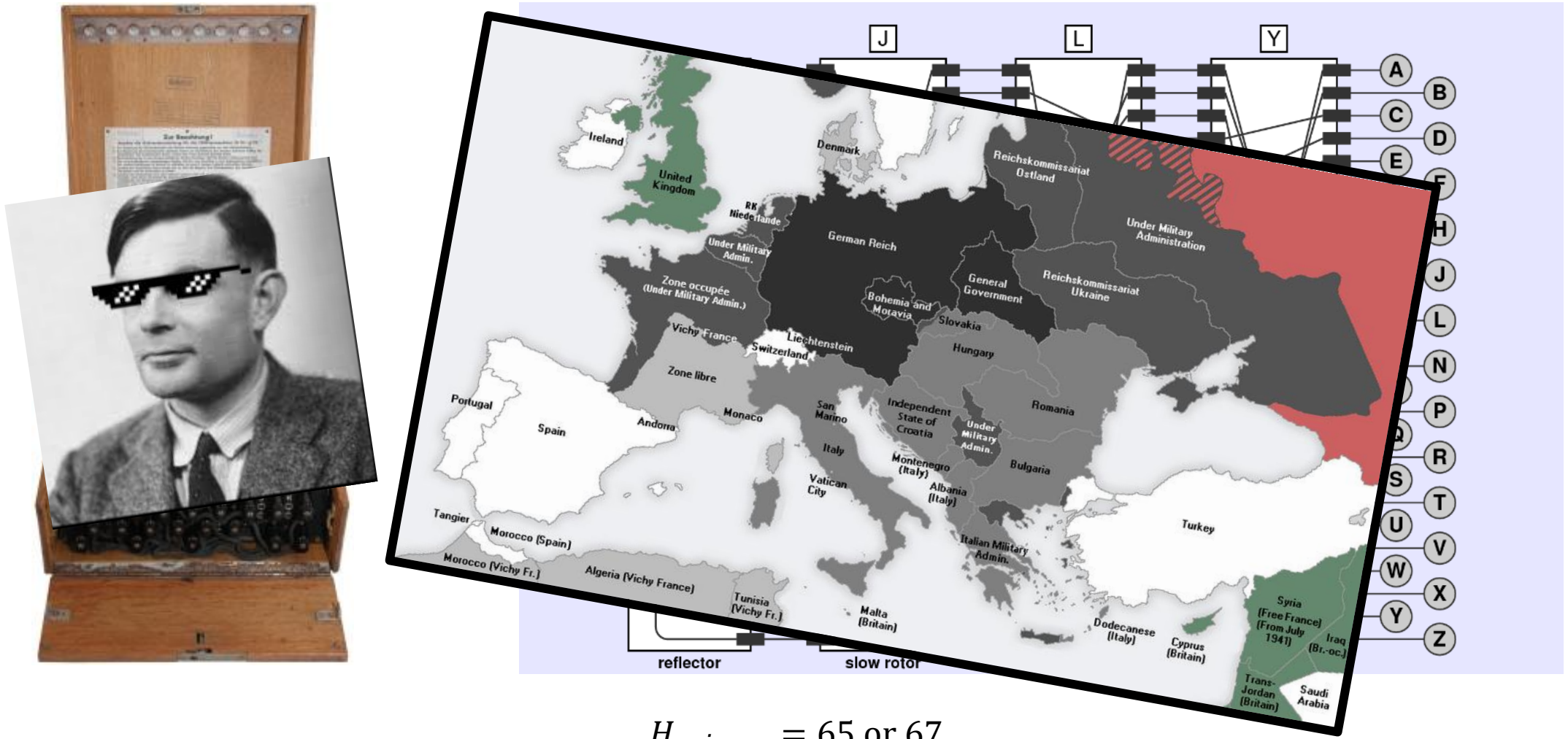
$$H_{enigma} = 65 \text{ or } 67$$

Enigma cipher machine



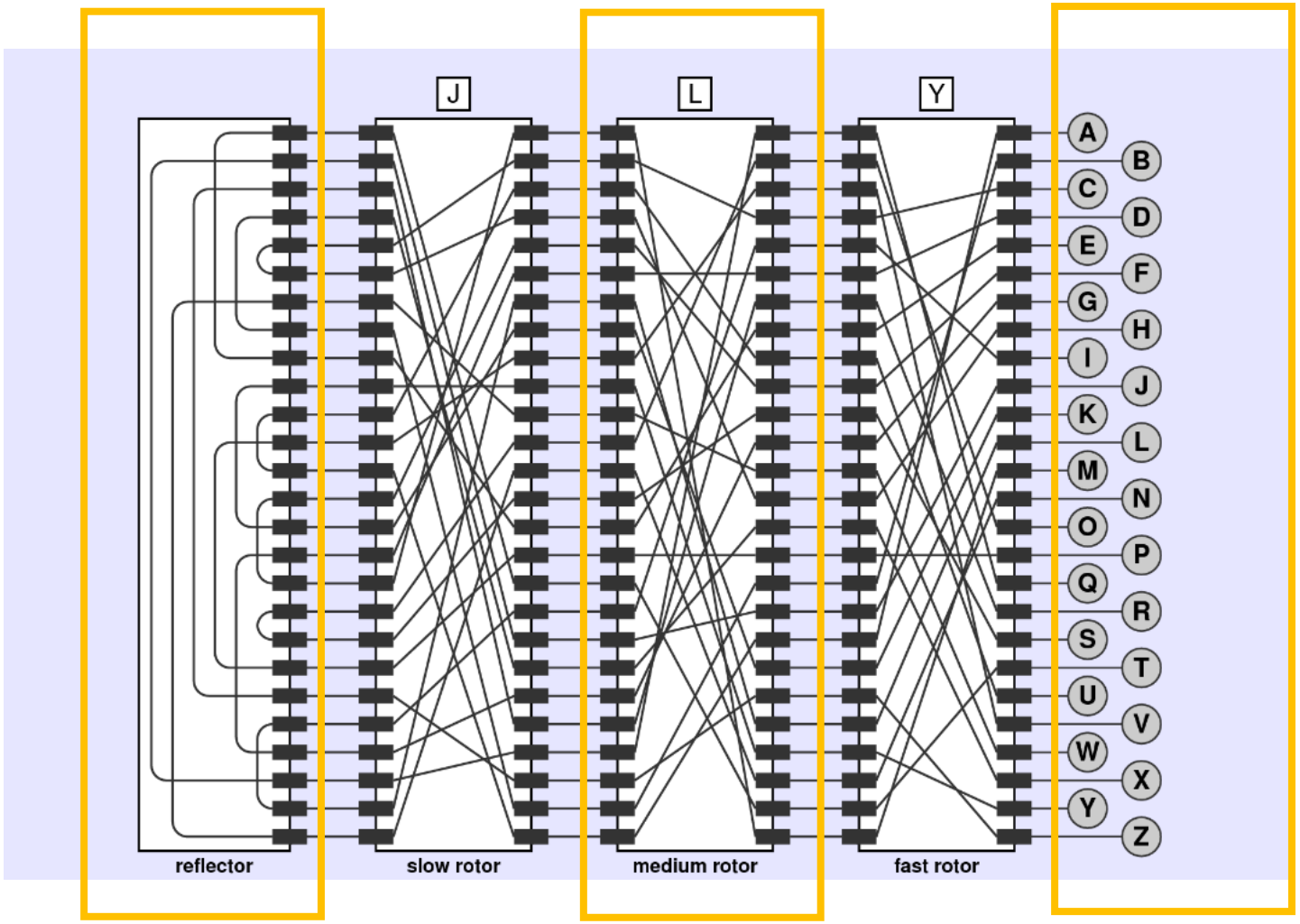
$$H_{enigma} = 65 \text{ or } 67$$

Enigma cipher machine



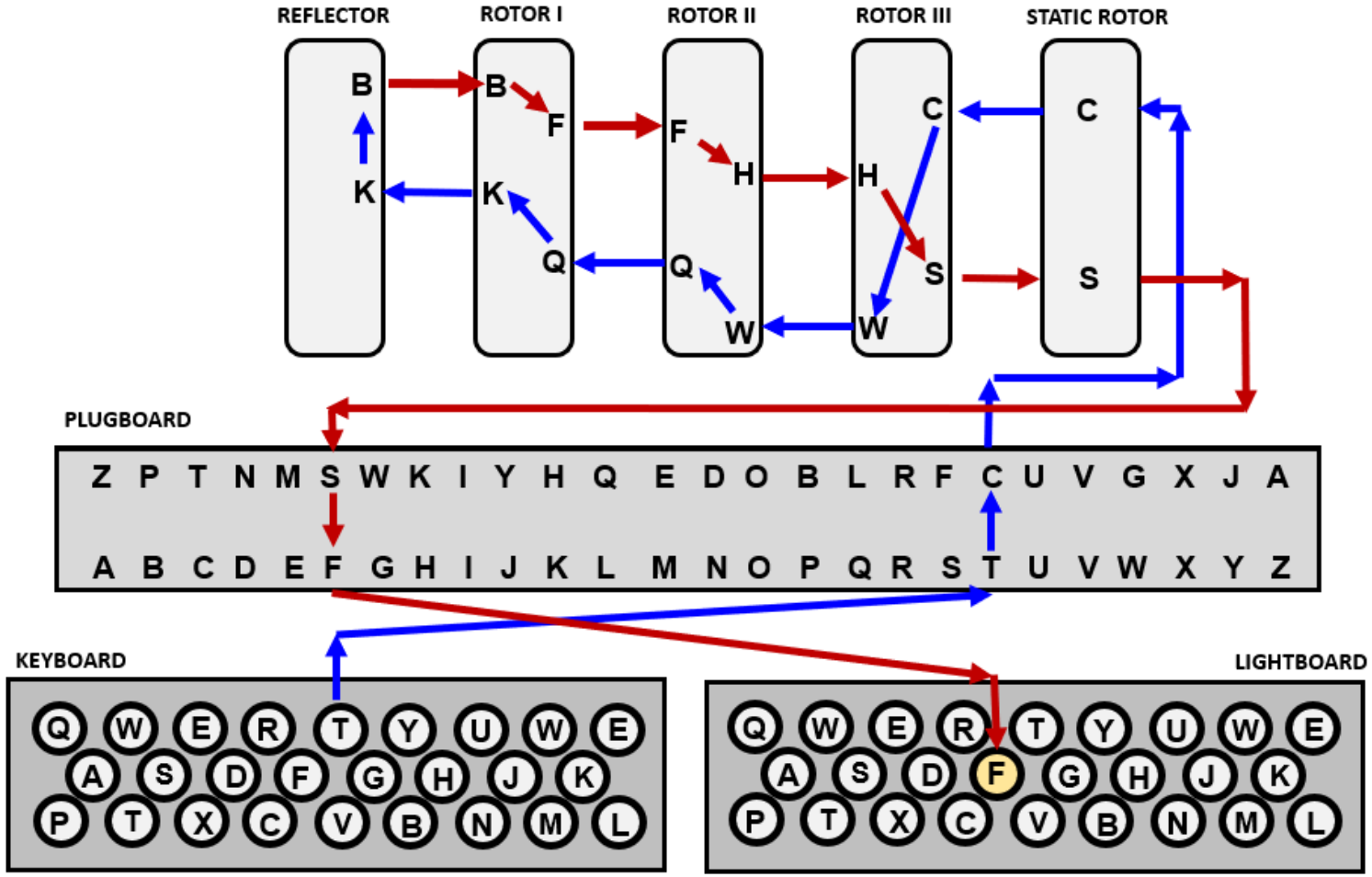
$$H_{enigma} = 65 \text{ or } 67$$

Enigma cipher machine



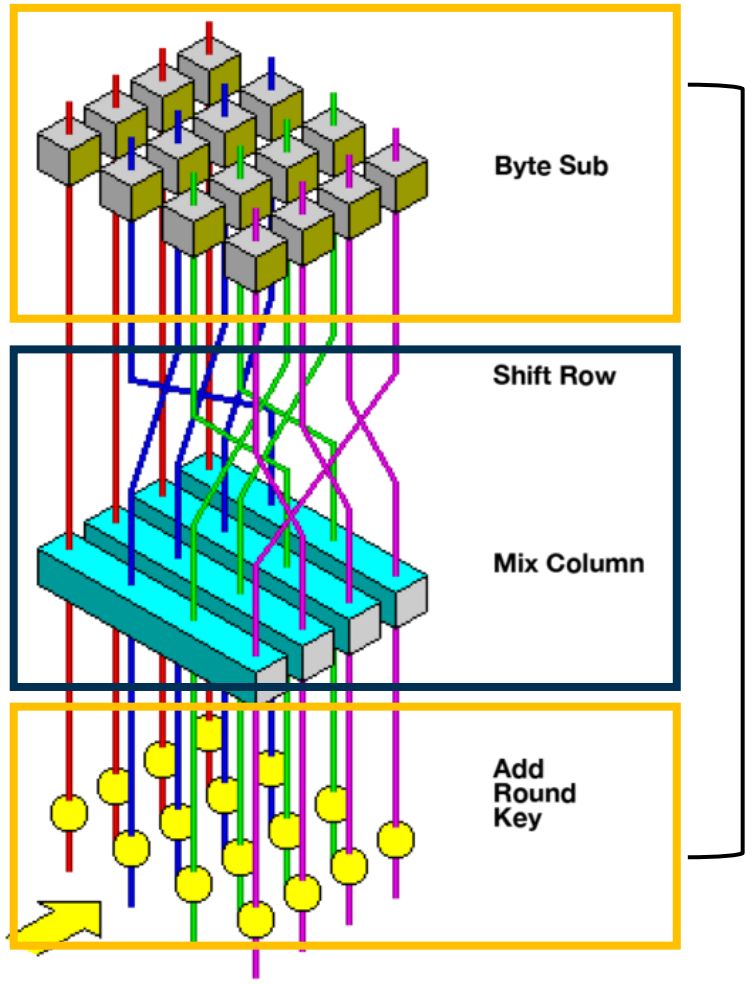
$$H_{enigma} = 65 \text{ or } 67$$

Enigma cipher machine



$$H_{enigma} = 65 \text{ or } 67$$

AES cipher



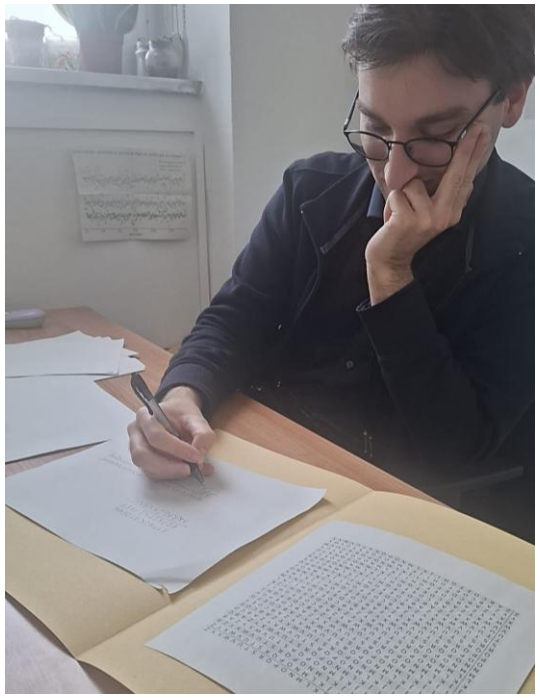
$\times$ 10 (or 12 or 14)

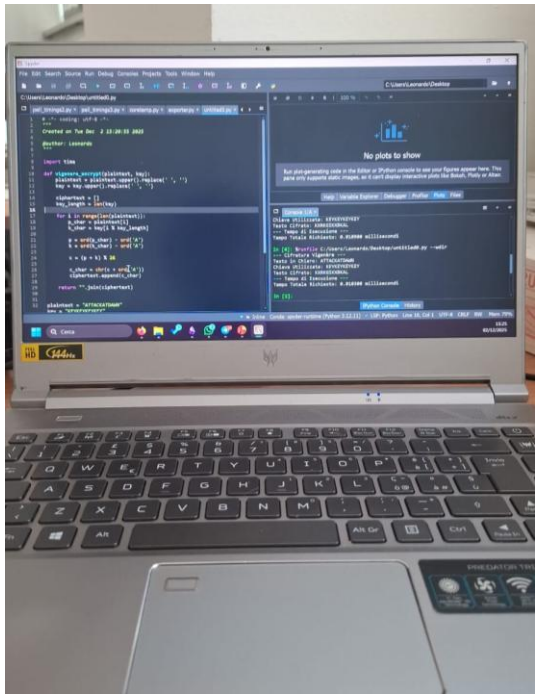
Confusion: each output character should depend on the key in a complex way.

Diffusion: each input character should influence many characters of the output, its statistical structure is dissipated.

$H_{AES} = 128 \text{ or } 192 \text{ or } 256$

Good news



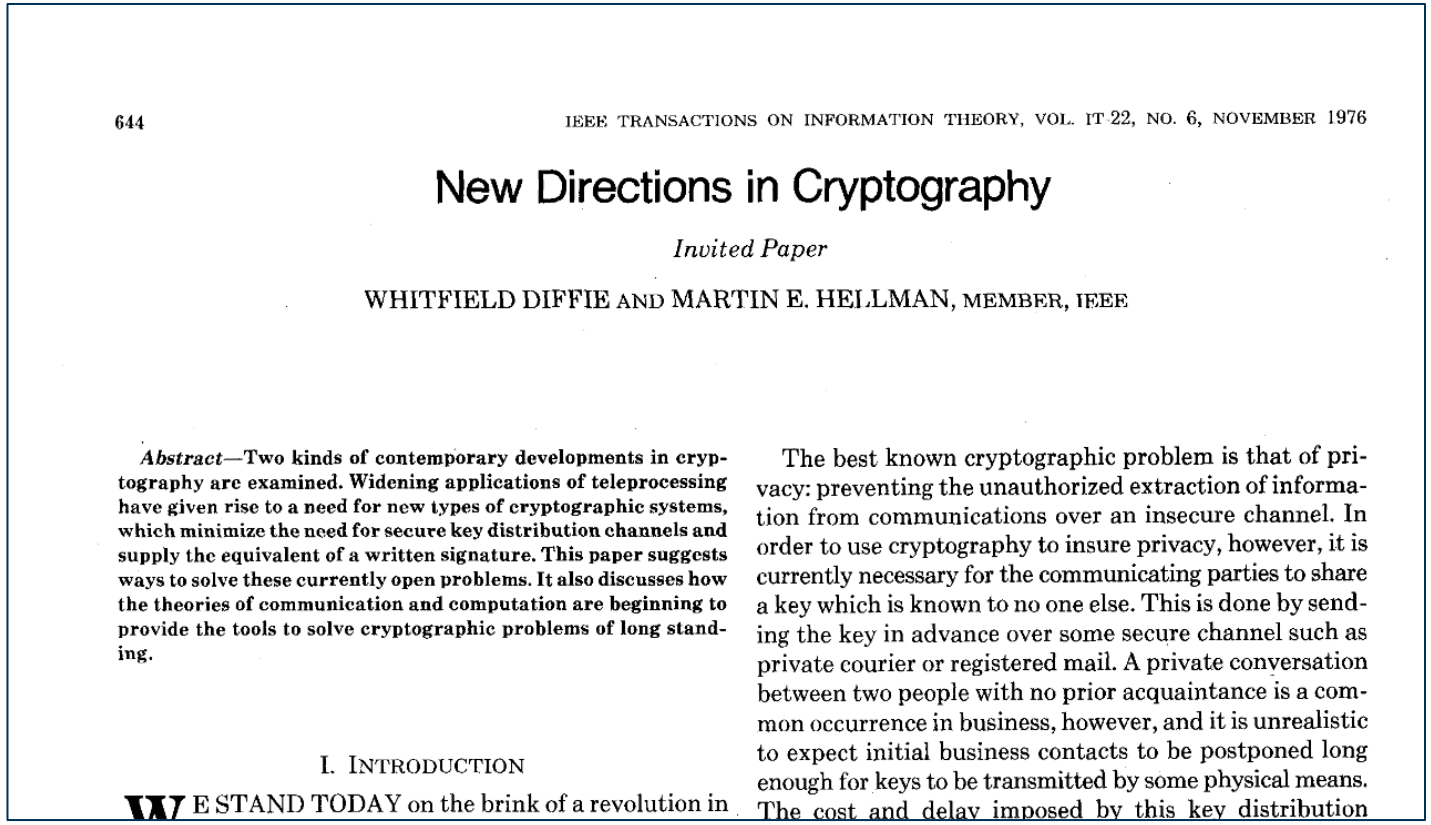


	me	**my laptop**
Vigenere	15 minutes	0.00001 seconds
AES-128	6 to 8 hours	0.00015 seconds

** benchmark on 128 characters*

Bad news

New fronteers



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

I. INTRODUCTION

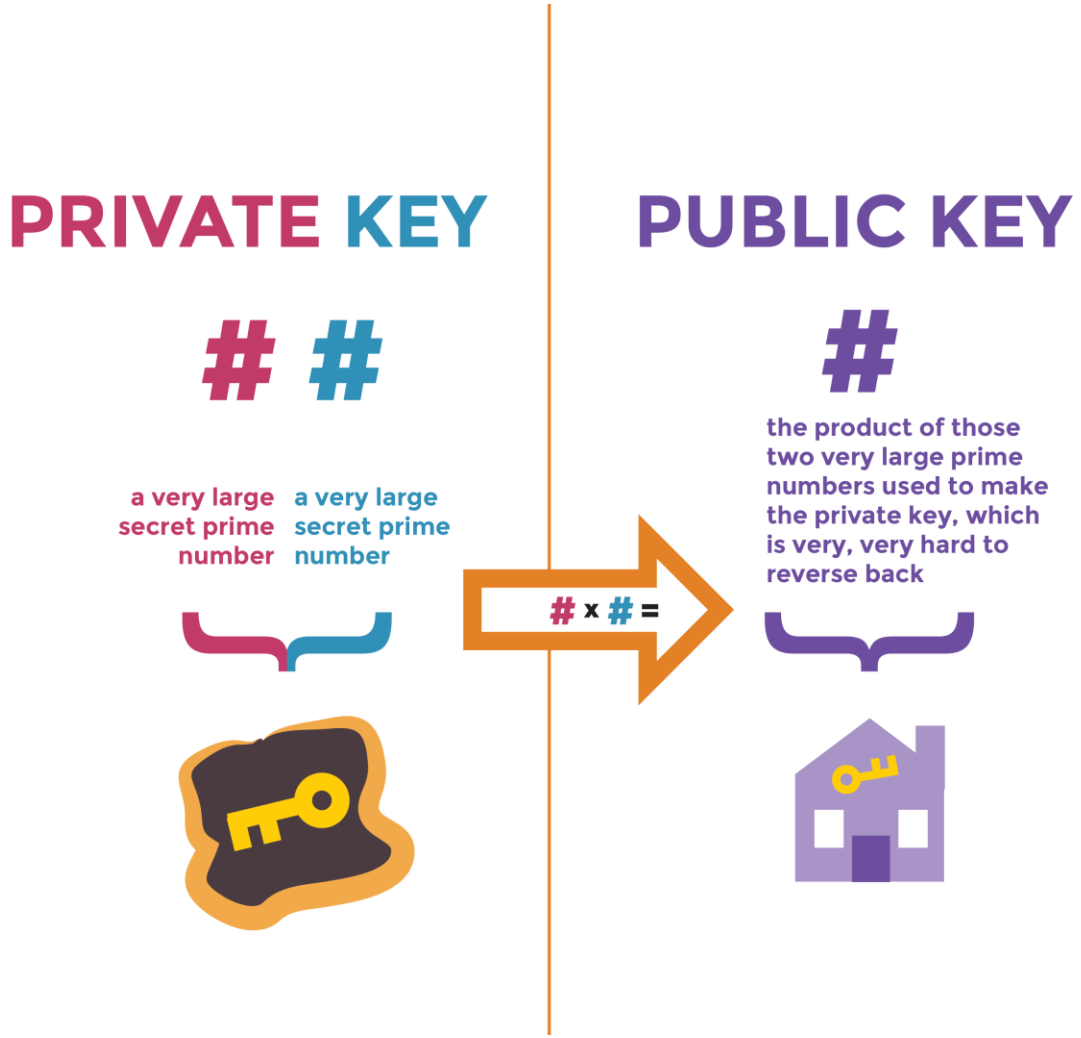
WE STAND TODAY on the brink of a revolution in

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution

"We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing [...]. At the same time, theoretical developments [...] show promise of providing provably secure cryptosystems, changing this ancient art into a science."

(W. Diffie, M. Hellman)

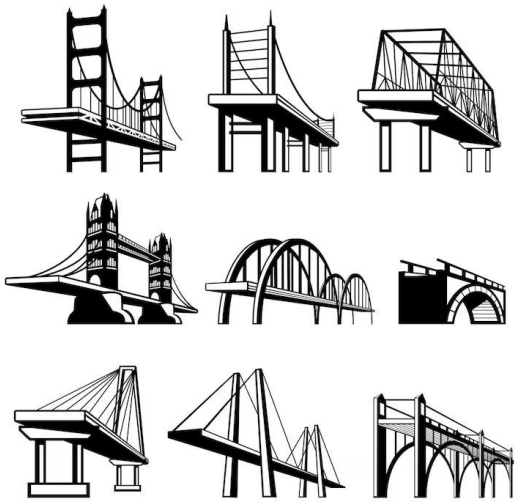
New fronteers 1: paradigms



New fronteers1: paradigms

- Block ciphers
- Hash functions
- Stream ciphers
- Signature schemes
- Zero knowledge proofs
- Key encapsulation mechanisms
- …

New fronteers: 2, security



New fronteers: 2, security

INTERLUDE: What Cryptography is Not (p2)


FANNY


ARTHUR


CORALINE


HIPPOLYTE

GWEN


AUGUSTIN


MAGGIE


ROGER


MARTIN


THEOPHILE


CAPUCINE


MAXIME

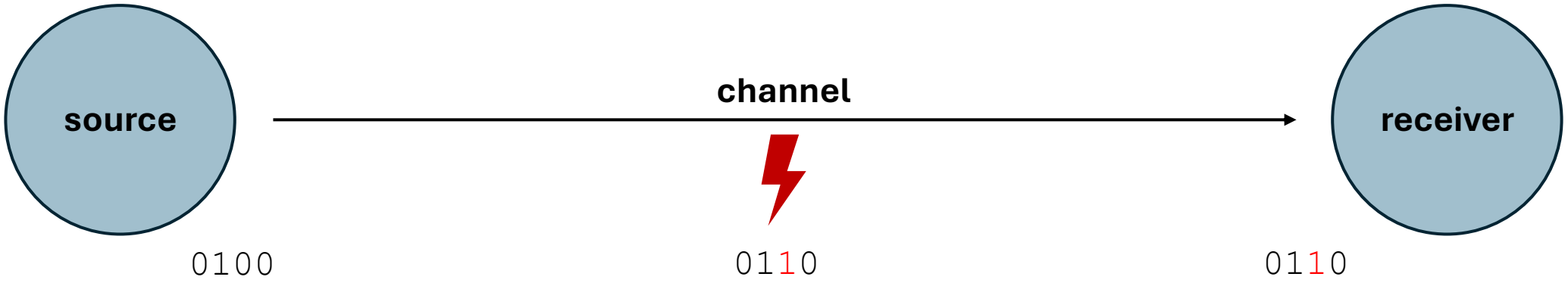

MELINA


ROBIN

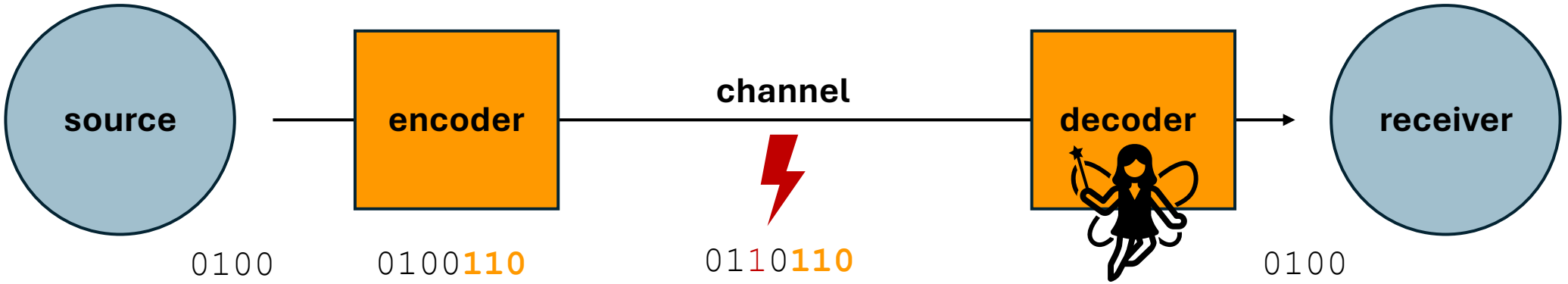

SANDRA


JUSTINE

Interlude: coding theory



Interlude: coding theory



A	alphabet
k	input length
n	code length

Interlude: coding theory

Hackaday

Cosmic Ray Flips Bit, Assists Mario 64 Speedrunner

The leading theory is that this bit flip was caused by a cosmic ray event, though the likelihood of such an event is exceedingly rare. It's...

17 feb 2021

BBC

Bit flips: How cosmic rays grounded a fleet of aircraft

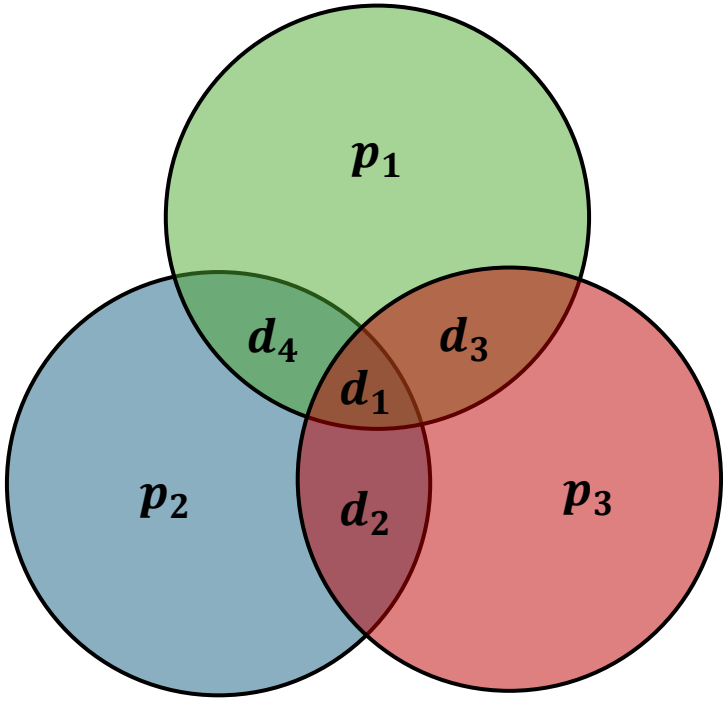
Radiation from space that led to more than 6000 Airbus aircraft needing emergency computer updates could become a growing problem.

1 dic 2025

“around one error per month per 256 MiB of RAM on a desktop computer”
(IBM, 1996)

Interlude: coding theory

0	0000000
1	0001011
2	0010101
3	0011110
4	0100110
5	0101101
6	0110011
7	0111000
8	1000111
9	1001100
10	1010010
11	1011001
12	1100001
13	1101010
14	1110100
15	1111111

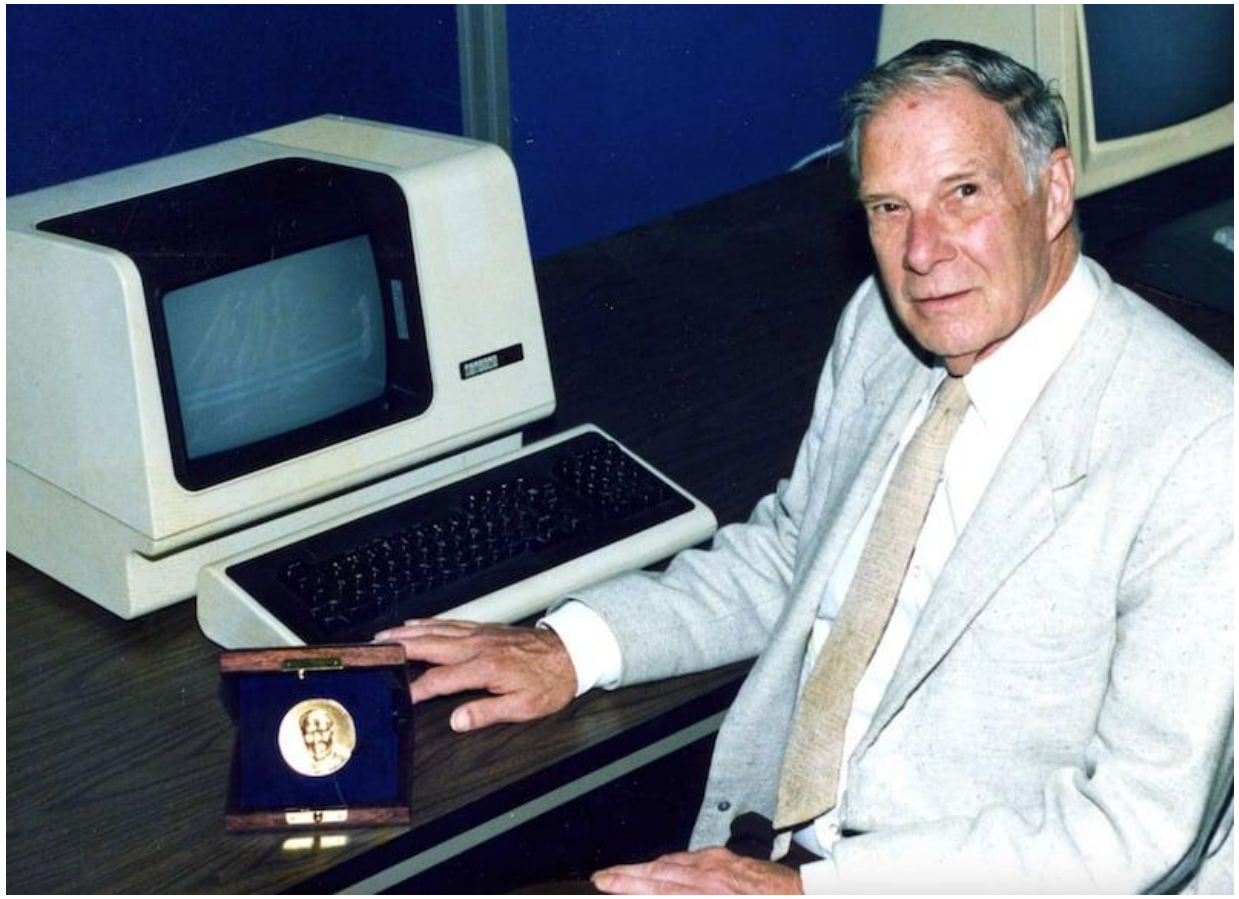


$$p_1 = d_1 + d_2 + d_4$$
$$p_2 = d_1 + d_3 + d_4$$
$$p_3 = d_2 + d_3 + d_4$$

Interlude: coding theory

0	0000000
1	0001011
2	0010101
3	0011110
4	0100110
5	0101101
6	0110
7	000
8	1000111
	1001100
10	1010010
11	1011001
12	1100001
13	1101010
14	1110100
15	1111111

[7,4] Hamming code



CAPUCINE

1010

CAPUCINE

1010101


0000000


0001111


0010011


0011100


CUMBIA!
0100101


0101010


0110110


0111001


1000110


1001001


1010101


1011010

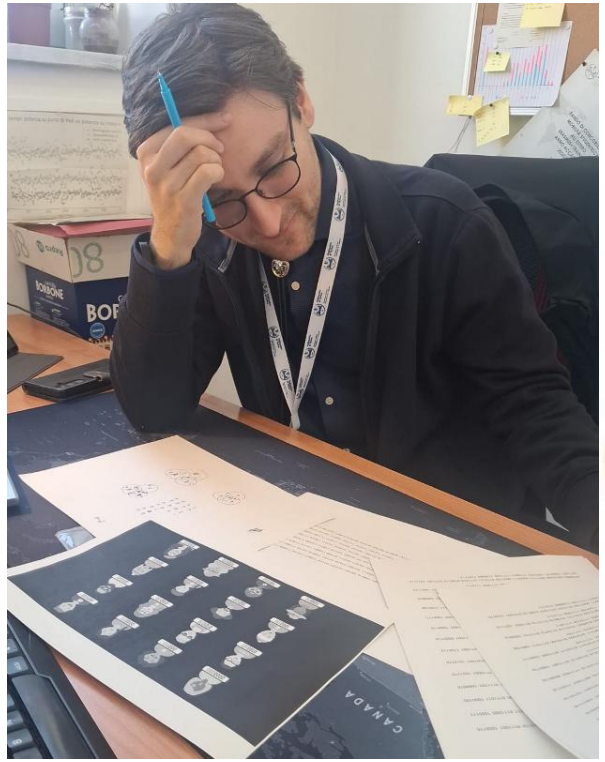

1100011


1101100


1110000


1111111

Interlude: coding theory



Me, decoding

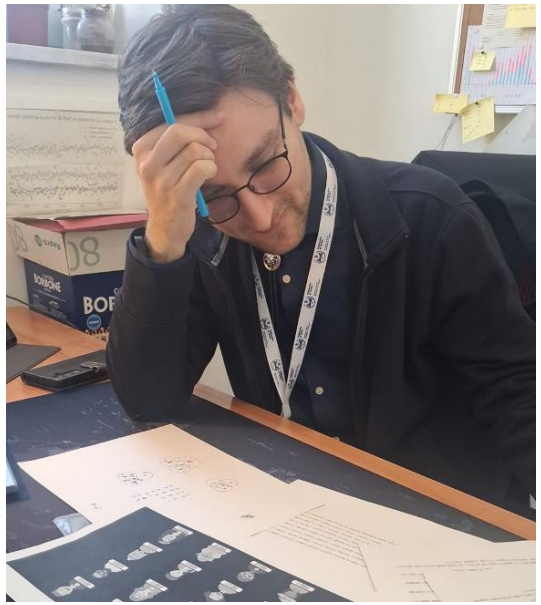
```
answer with 'y' for Yes or 'n' for No:
1. Hat? 1
2. Glasses? 0
3. Is sad? 1
4. Moustache? 0
5. Drawing on shirt? 1
6. Blue shirt/garment? 1
7. Dark hair? 1
Lie detected at question 6!
Identified Person: CAPUCINE

Do you want to play again? (y/n):
```

My laptop, decoding

Take aways

- Ciphers are now tailored for machines
- New directions: paradigms, security
- Cryptography ≠ coding theory
- Mathematics is not stressful at all

Encrypting (Dec. 2025)



Decoding (Feb. 2026)

1. Against entropy…
2. Machines themselves…
3. Contend in vain?

Human error: Enigma

- Simple keys

```
AAA, ABC, CIL
```

Human error: Enigma

- Simple keys
- Repeated messages

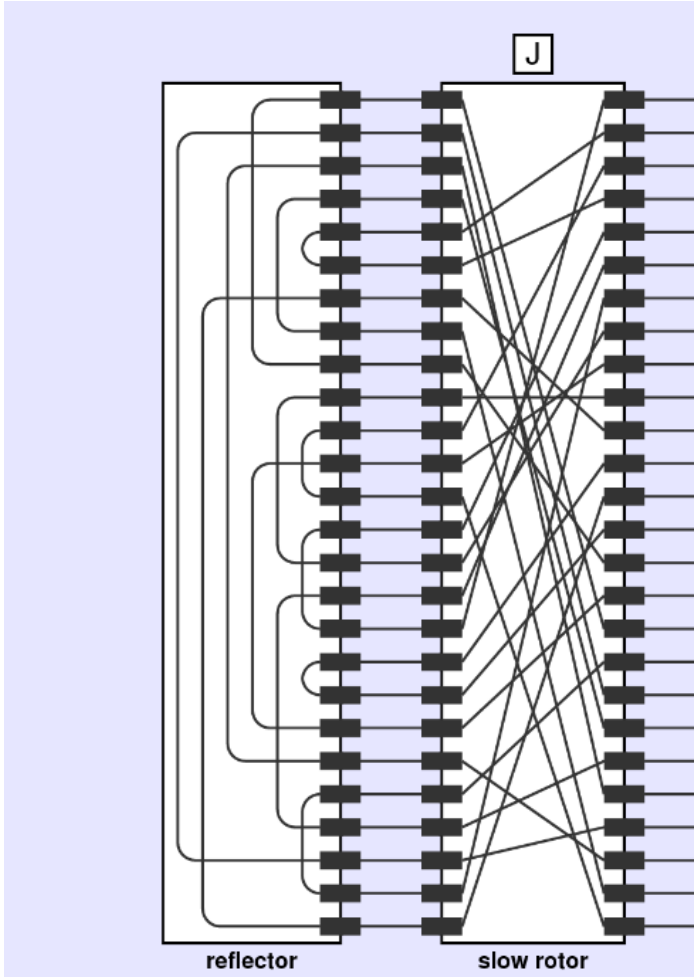
«Wetter für die Nacht..»

Human error: Enigma

- Simple keys
- Repeated messages
- Short messages

Human error: Enigma

- Simple keys
- Repeated messages
- Short messages
- Reflector (!)



Human error: Sony PS3

signature s
public key pk

secret key sk

Human error: Sony PS3

secret key sk


```
C5 B2 BF A1 A4 13 DD 16 F2 6D
31 C0 F2 ED 47 20 DC FB 06 70
```

Government Backdoors 101

What?

Any method to bypass security layers

Government Backdoors 101

What?
Any method to bypass security layers

Why?
National security, law enforcement

The four horsemen of infocalypse: drug-dealers, money-launderers, terrorists, and pedophiles.

Government Backdoors 101

What?
Any method to bypass security layers

Why?
National security, law enforcement

Are they ethical?
Who knows, probably not much

The four horsemen of infocalypse: drug-dealers, money-launderers, terrorists, and pedophiles.

Government Backdoors 101

What?
Any method to bypass security layers

Why?
National security, law enforcement

Are they ethical?
Who knows, probably not much

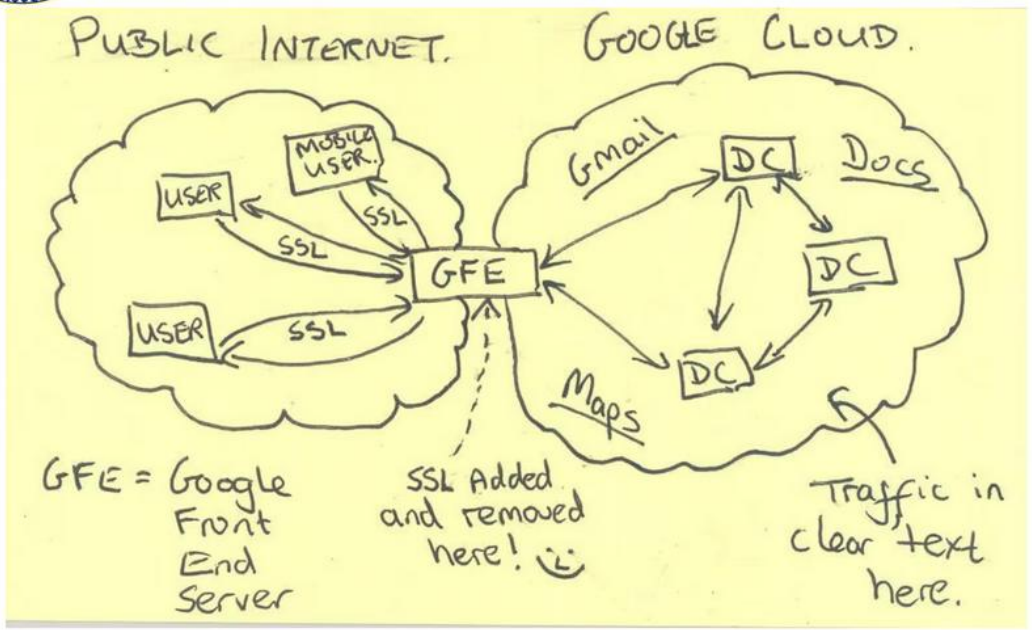
Are they safe?
No

The four horsemen of infocalypse: drug-dealers, money-launderers, terrorists, and pedophiles.

Government Backdoors 101

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

This will try to be as objective as possible.
Still, it's hard to be objective when NSA slides look like this.

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

1970: CIA & BND buy CryptoAG via shell companies

CIA + Bundesnachrichtendienst

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

1970: CIA & BND buy CryptoAG via shell companies

HAGELIN-CRYPTOS

CRYPTO AG

=

CENTRAL INTELLIGENCE AGENCY

UNITED STATES OF AMERICA

+

BND

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

1970: CIA & BND buy CryptoAG via shell companies

HAGELIN-CRYPTOS

CRYPTO AG

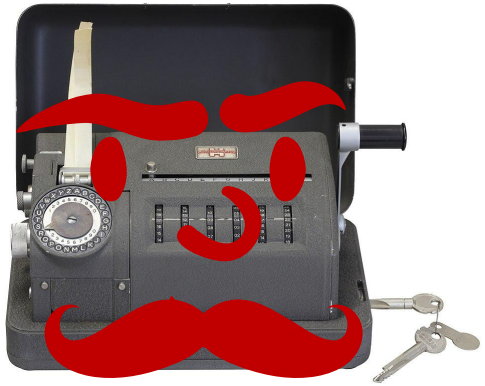
=

CENTRAL INTELLIGENCE AGENCY

UNITED STATES OF AMERICA

+

BND



Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

1970: CIA & BND buy CryptoAG via shell companies

1991: IRAQ takes Hans Bühler hostage

HAGELIN-CRYPTOS

CRYPTO AG

=

CENTRAL INTELLIGENCE AGENCY

UNITED STATES OF AMERICA

+

BND

Backdoors: Operation Rubicon

1951: Boris Hagelin meets NSA

1952: Boris Hagelin founds CryptoAG

1970: CIA & BND buy CryptoAG via shell companies

1991: IRAQ takes Hans Bühler hostage

1994: Hans Bühler spills the beans

HAGELIN-CRYPTOS

CRYPTO AG

=

CENTRAL INTELLIGENCE AGENCY

UNITED STATES OF AMERICA

+

BND

Backdoors: Operation Rubicon

1973: US coup in Chile
1978: Egypt-Israel Camp David Accords
1982: Falklands war
1986: US attacks on Libia (Operation El Dorado Canyon)
1989: US invasion of Panama (Operation Just Cause)

+ *many, many domestic events*

Backdoors: Operation Rubicon

America
Argentina
Brazil
Chile
Colombia
Honduras
Mexico
Nicaragua
Peru
Uruguay
Venezuela

Europe
Austria
Belgium
Czechoslovakia
Greece
Hungary
Ireland
Italy
Portugal
Romania
Spain
Türkiye
Vatican City
Yugoslavia

Africa
Algeria
Angola
Congo
Egypt
Gabon
Ghana
Guinea
Ivory Coast
Libya
Mauritius
Morocco
Nigeria
South Africa
Sudan
Tanzania
Tunisia
Zaire
Zimbabwe

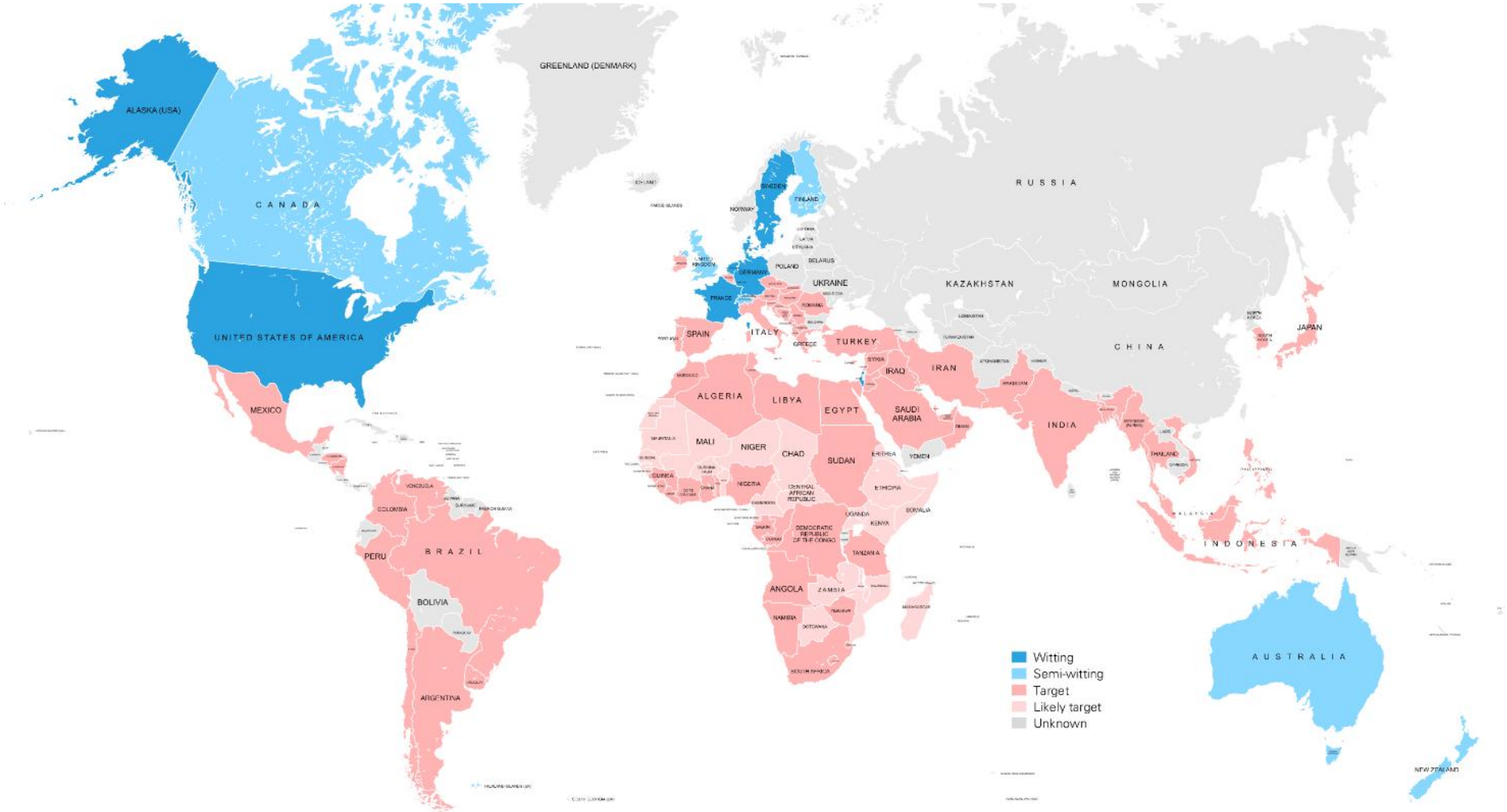
Middle East
Iran
Iraq
Jordan
Kuwait
Lebanon
Oman
Qatar
Saudi Arabia
Syria
U.A.E.

Asia
Bangladesh
Burma
India
Indonesia
Japan
Malaysia
Pakistan
Phillipines
South Korea
Thailand
Vietnam

Organisations
United Nations

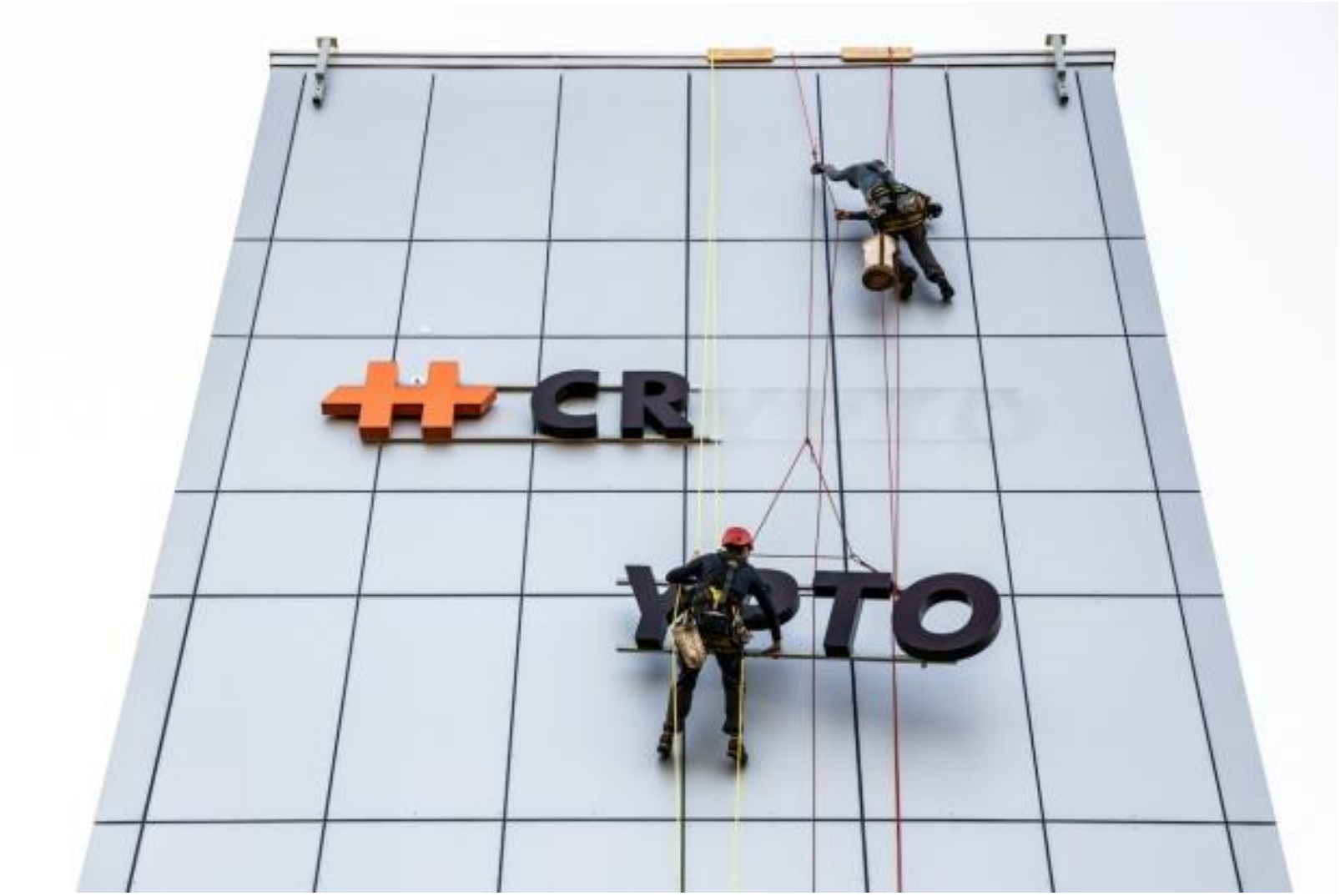
"The Intelligence Coup of the Century"
- CIA

Backdoors: Operation Rubicon



"The Intelligence Coup of the Century"
- CIA

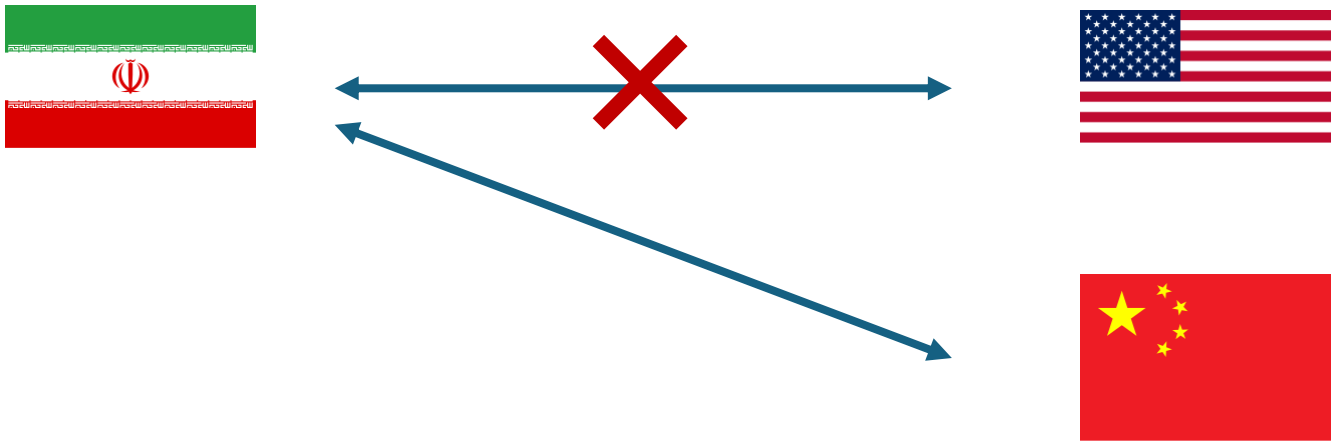
Backdoors: Operation Rubicon



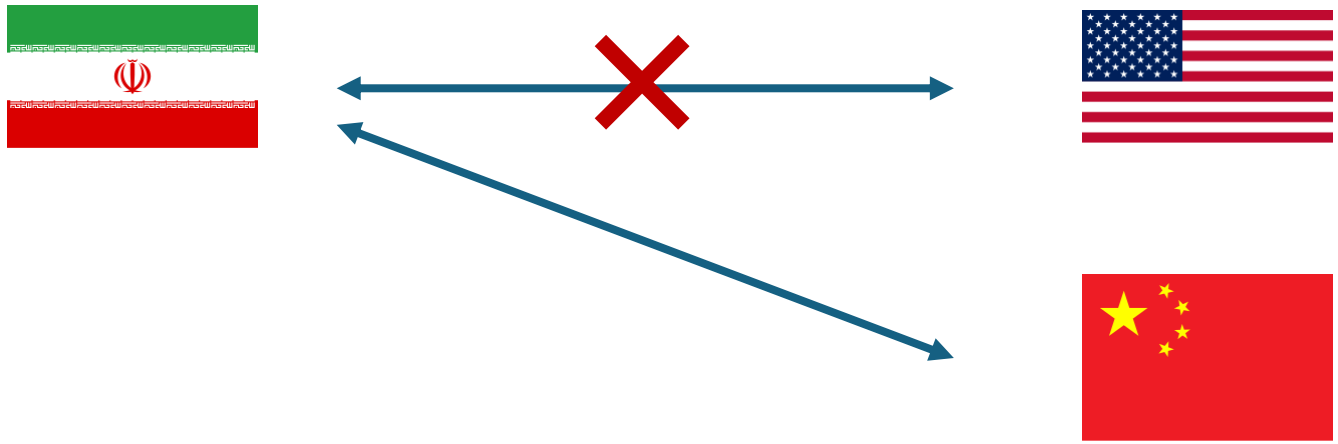
Backdoors: Operation Rubicon

Italian traffic was reportedly still being deciphered around 2001.

Backdoors backfire: Operation Shotgiant

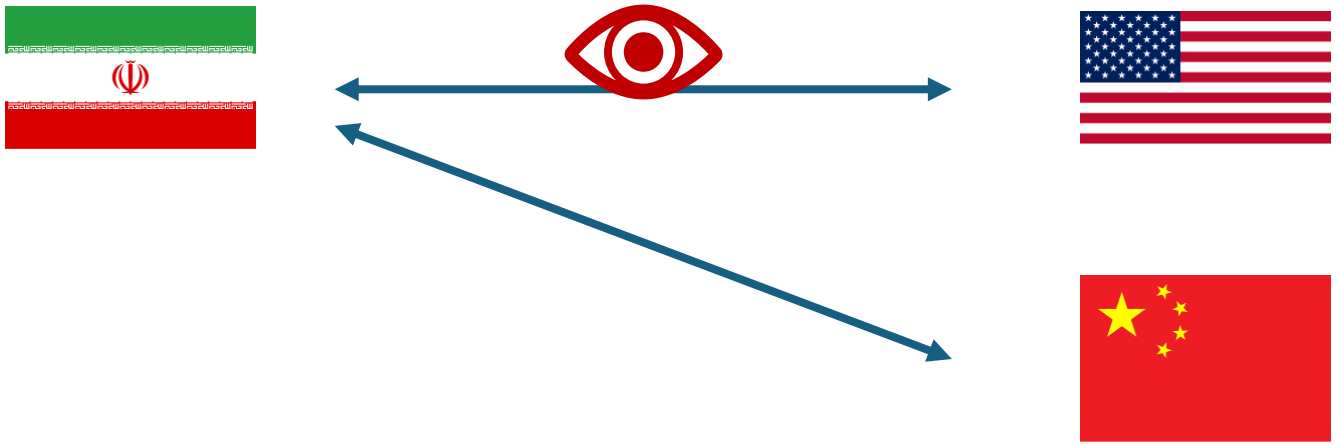


Backdoors backfire: Operation Shotgiant



«lawful intercept backdoors»

Backdoors backfire: Operation Shotgiant



«lawful intercept backdoors»

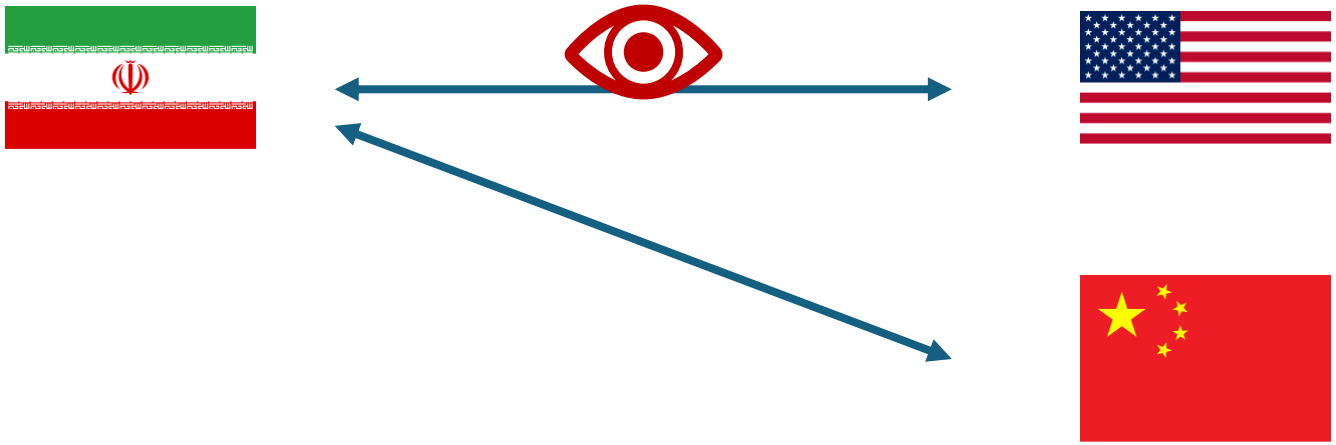
The Hacker News

NSA Hacked Servers of Chinese telecom Huawei, Stole Source Codes

Operation Shotgiant: NSA Hacked Chinese telecom Huawei and Stole Product Source Codes to write exploits.

23 mar 2014

Backdoors backfire: Operation Shotgiant



«lawful intercept backdoors»

[…] this is both curious and puzzling. Have you ever seen a thief in the street who advertises […] that he is a thief? Honestly speaking, I think what the U.S. has done here cannot be accepted as correct.

- Hua Chunying, Foreign Ministry spokeperson

CryptoWars™

1991: Phil Zimmerman & PGP

- Cryptography is a weapon, export prohibited
- Source code printed on books
- Case closed in 1996 thanks to public pressure

1999: Bernstein vs United States

- Publishing is protected by 1st emendament

Conclusion: pyrrhic victory

- Cryptography can be exported, but…
- RSA export limited to weak keys

Backdoors: NSA & DualEC

2006: NSA proposes a PRNG algorithm for adoption
2007: Shumow & Ferguson find something that *looks like a backdoor*

"we're not saying NSA did this, but…"

The Main Point

- If an attacker knows *d* such that *d*P = Q* then they can easily compute *e* such that *e*Q = P* (invert mod group order)
- If an attacker knows *e* then they can determine a small number of possibilities for the internal state of the Dual Ec PRNG and predict future outputs.
- We do not know how the point *Q* was chosen, so we don't know if the algorithm designer knows *d* or *e*.

Conclusion

- WHAT WE ARE NOT SAYING:
  NIST intentionally put a back door in this PRNG
- WHAT WE ARE SAYING:
  The prediction resistance of this PRNG (as presented in NIST SP800-90) is dependent on solving one instance of the elliptic curve discrete log problem.
  (And we do not know if the algorithm designer knew this before hand.)

Backdoors: NSA & DualEC

2006: NSA proposes a PRNG algorithm for adoption
2007: Shumow & Ferguson find something that *looks like a backdoor*

> *“we're not saying NSA did this, but…”*

2013: Post-Snowden, RSA Security admits getting USD 10Mln from NSA to adopt it

Backdoors: NSA & DualEC

“If you can’t beat them, trick them!”
- NSA, probably

Backdoors: NSA & DualEC
Backdoors: NSA & DES

“If you can’t beat them, trick them!”
- NSA, probably

Backdoors: NSA & DualEC
Backdoors: NSA & DES
Backdoors: NSA & AES

“If you can’t beat them, trick them!”
- NSA, probably

Backdoors: NSA & post-quantum? (probably not)

CRYPTOGRAPHY

A very unscientific guide to the security of various PQC algorithms

By Sophie Schmieg December 13, 2025 No Comments

Backdoors: Chat Control

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse”

Either

- Break/weaken E2E ← not a great idea
- Client-side scanning ← technically a spyware

Backdoors: Chat Control

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse”

For: **307**. Against: **306**. Abstentions: **24**. In total, **637 MEPs** voted. **81 MEPs** didn’t vote.

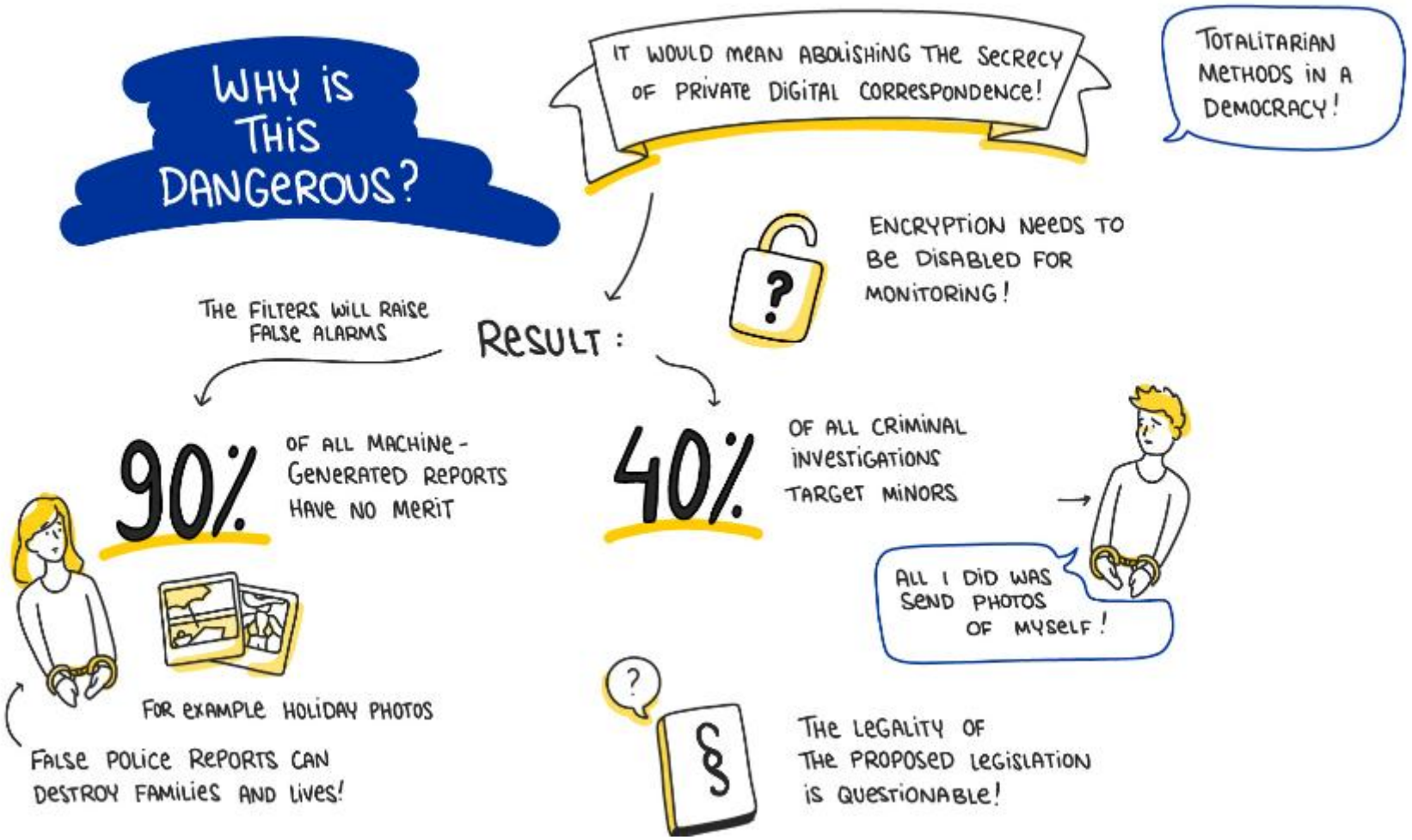
Backdoors: Chat Control

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse”

@ Patrick Breyer

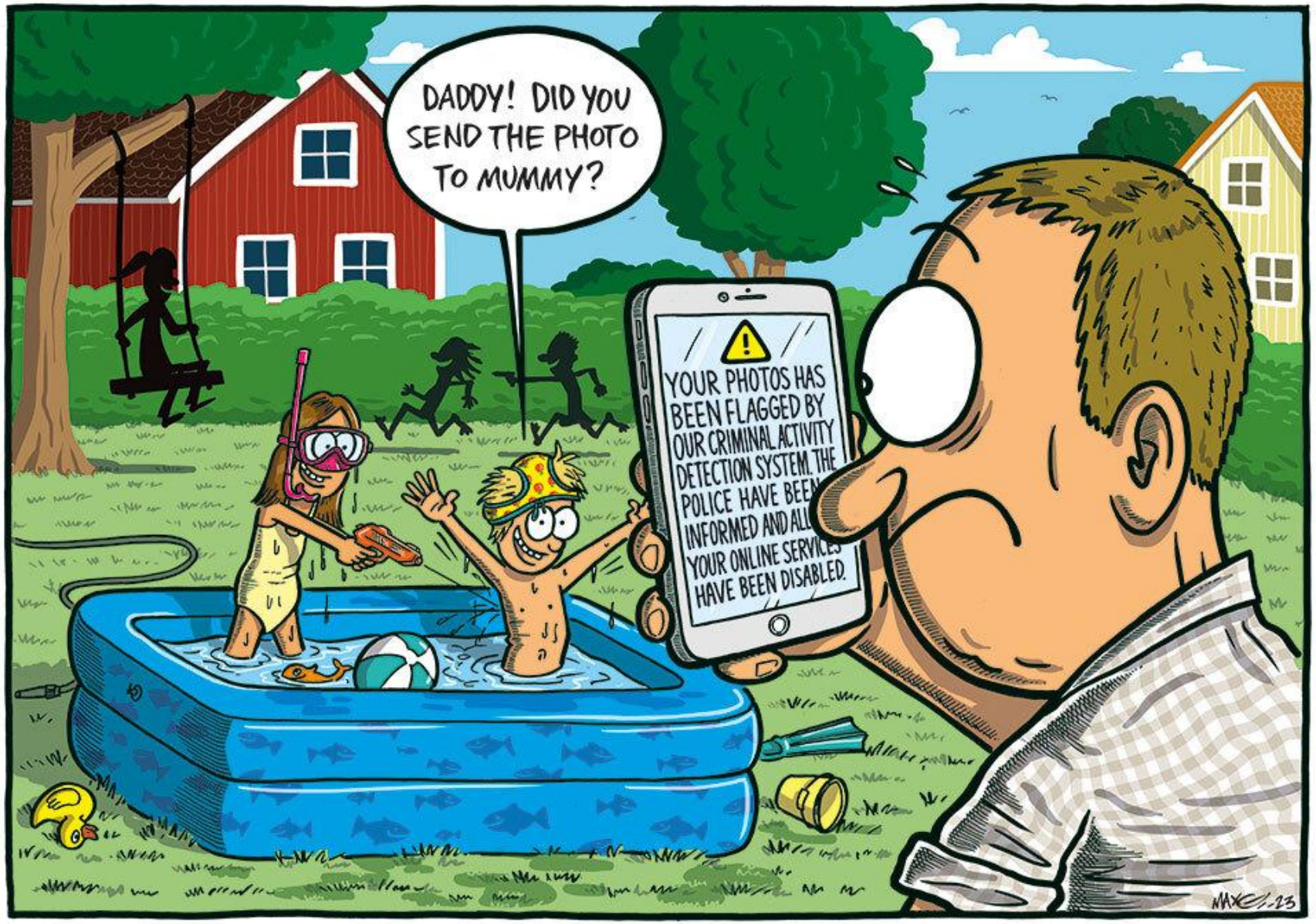
Backdoors: Chat Control

“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse”



@ Patrick Breyer

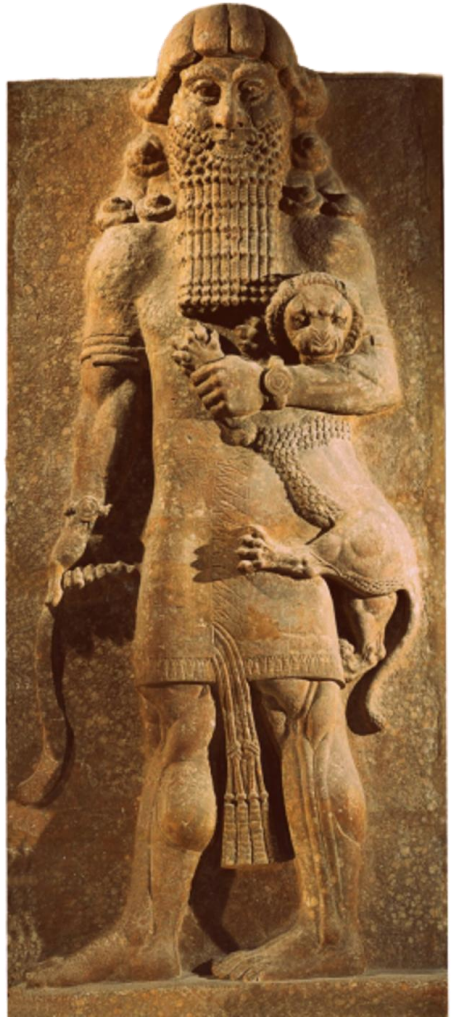
Backdoors: Chat Control



Take aways

- Humans are bad at following protocols. Really bad.
- Tension between surveillance and privacy
- How secure can cryptography be?

“Get in, fair reader, into the depths of Cryptography.
Inspect the theory, view its foundations.
Is not the very core made of fine mathematics?”
- ***Gilgamesh***



A seminar on the history of cryptography, in the historical city of Turin.

HisTo26 explores the evolution of secret writing, from Classical and Renaissance ciphers to World War II cryptanalysis and the cold war. Topics include: evolution of cryptography, historical ciphers, analysis of documents and cases of study.

Organisers: Paolo Bonavoglia (DeCifris), Leonardo Errati (PoliTo).

Invited speakers:

Dr. Dermot Turing
Visiting Fellow
Kellow College, Oxford

Prof. Joachim Rosenthal
Professor of Mathematics
University of Zurich

Flavio Atzeni
Chief Warrant Officer
Italian CC (retired)

Dr. Francesco Cosimato
Brigadier General
Italian Army (retired)

With the contribution of BitPolito and Disma.
http://sites.google.com/view/histo26/home

Politecnico di Torino

BitPolito

Politecnico di Torino
Department of Mathematical Sciences "G. L. Lagrange"

histo 2026