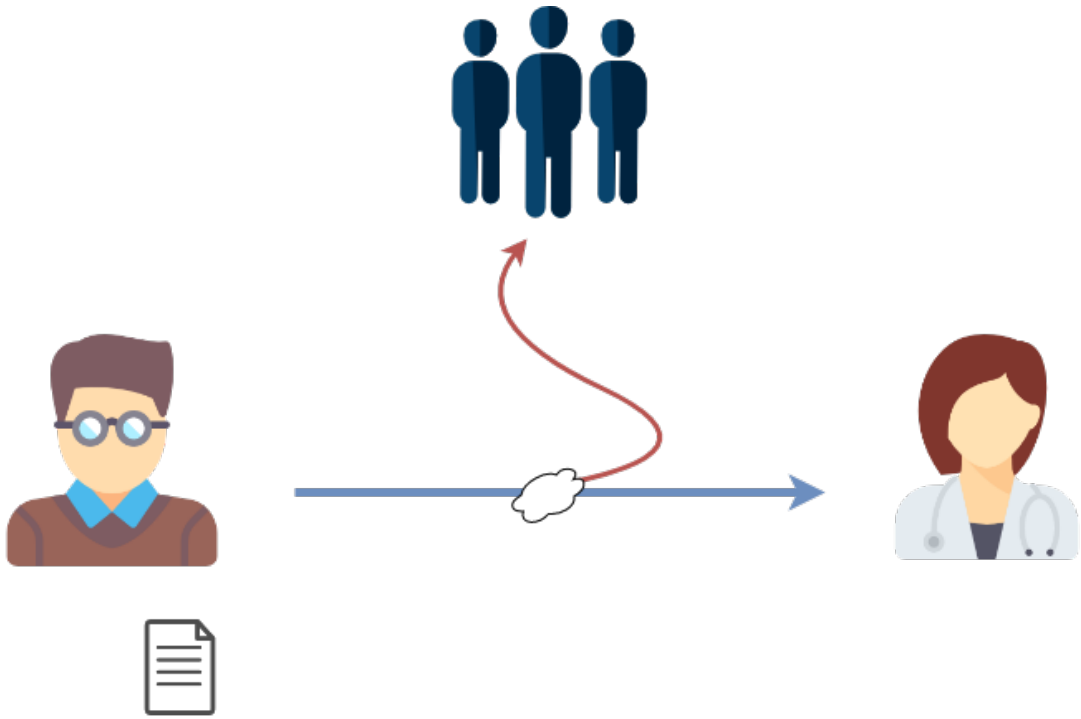
Pensamiento Criptográfico y Nuevos Protocolos

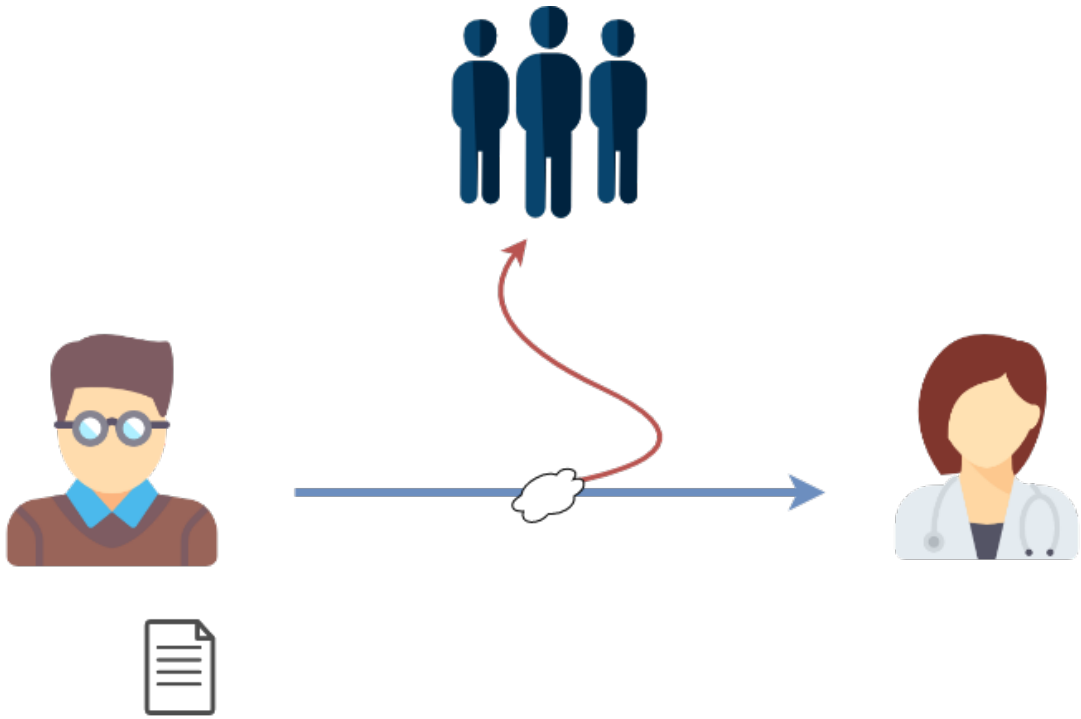
Francisco Vial

11 de Junio, 2019

Fundamentos
de los datos

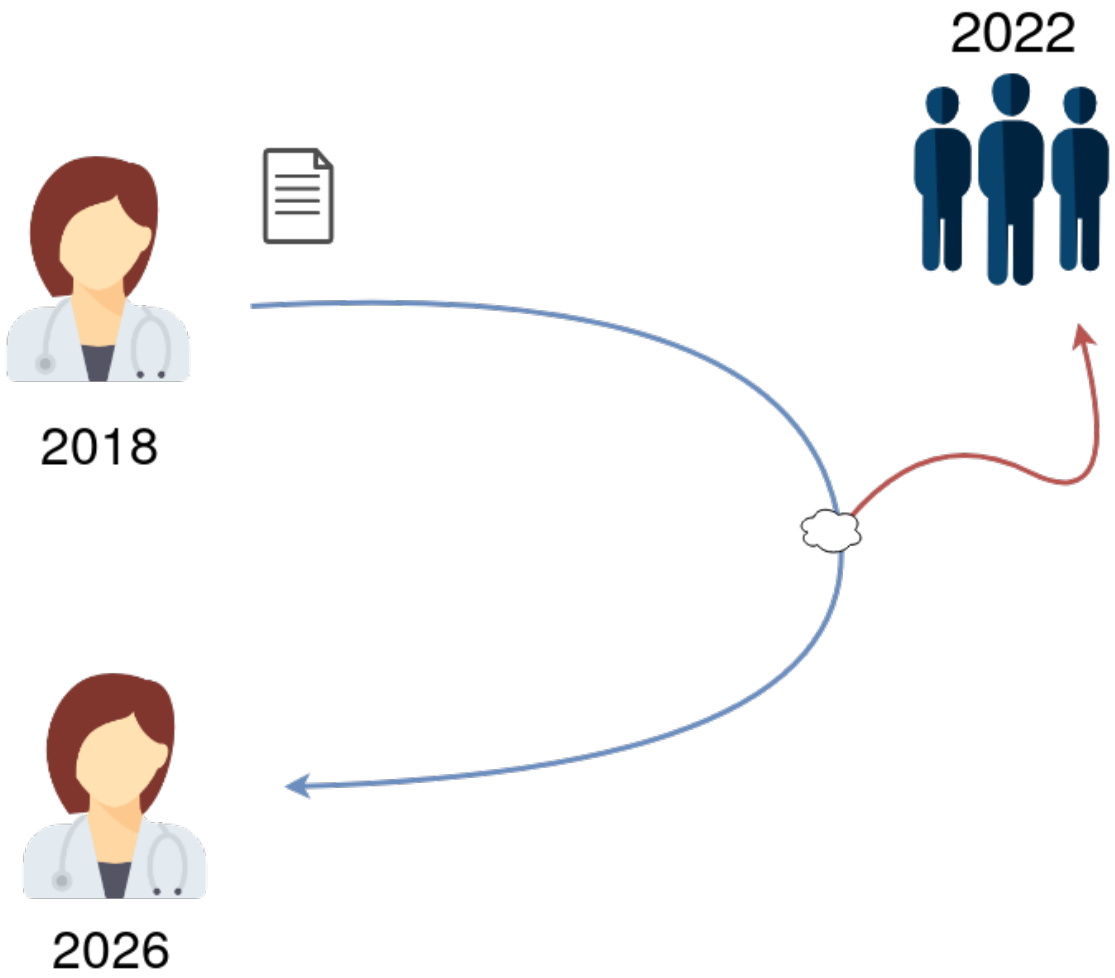


... not only this!



... not only this!

Not only this:



I swear I'm Alice!

And I commit to this document exactly.

... and not only this!

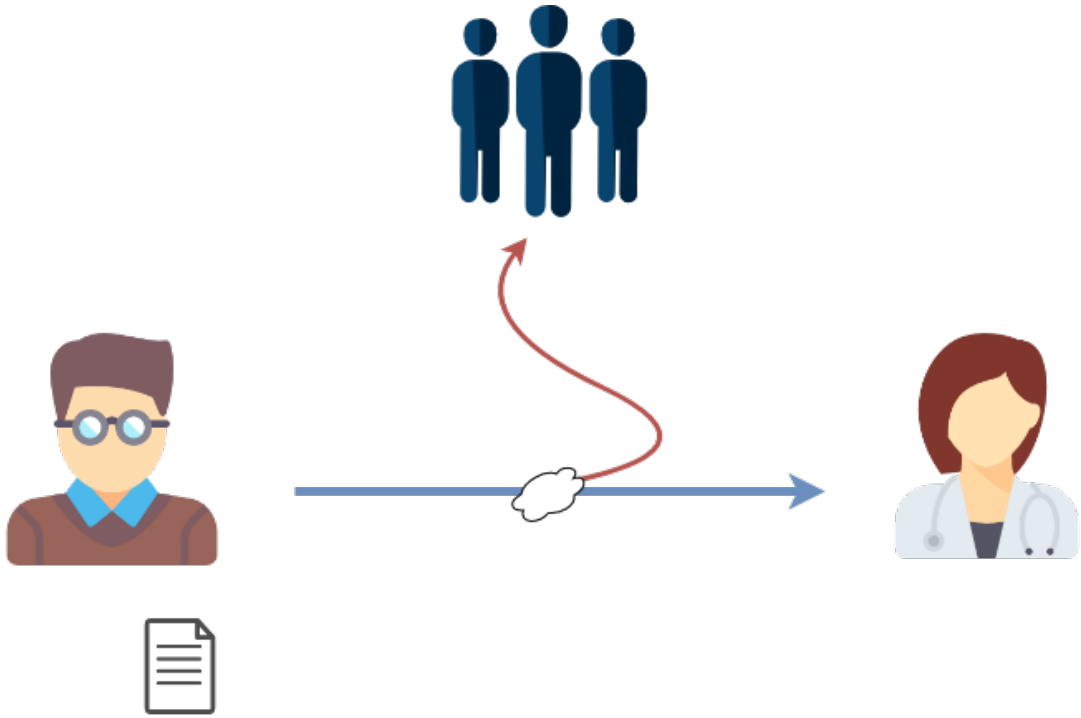
I swear I'm Alice!

And I commit to this document exactly.

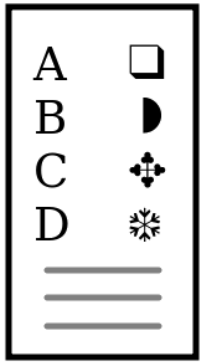
... and not only this!

... and certainly not only this!

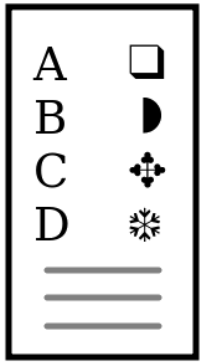
Kryptos - Graphias

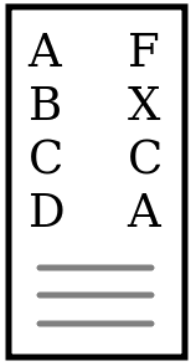


Substitution, polyalphabetic

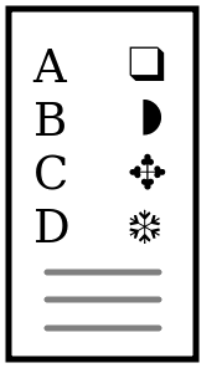


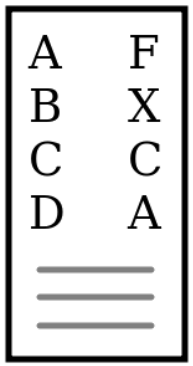
Substitution, polyalphabetic



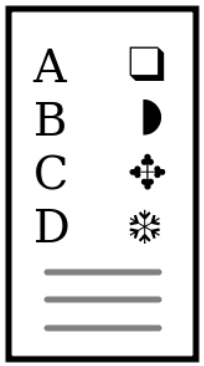


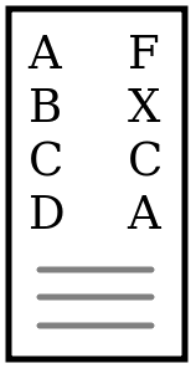
Substitution, polyalphabetic





Substitution, polyalphabetic



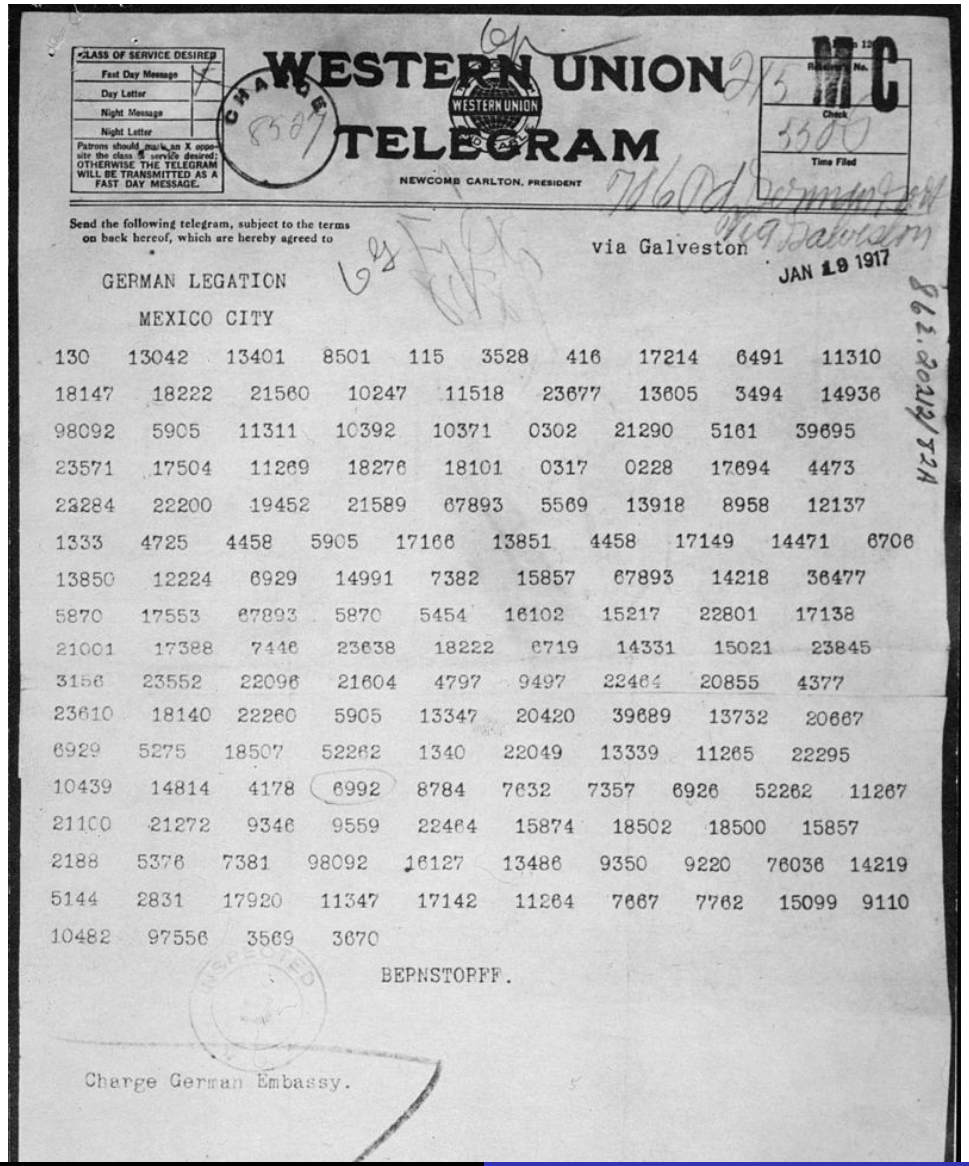


KEYWORD: TURING

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	Q
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	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	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	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	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	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	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	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

Historic Interlude – WWI, WWII

The Zimmermann Telegram



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

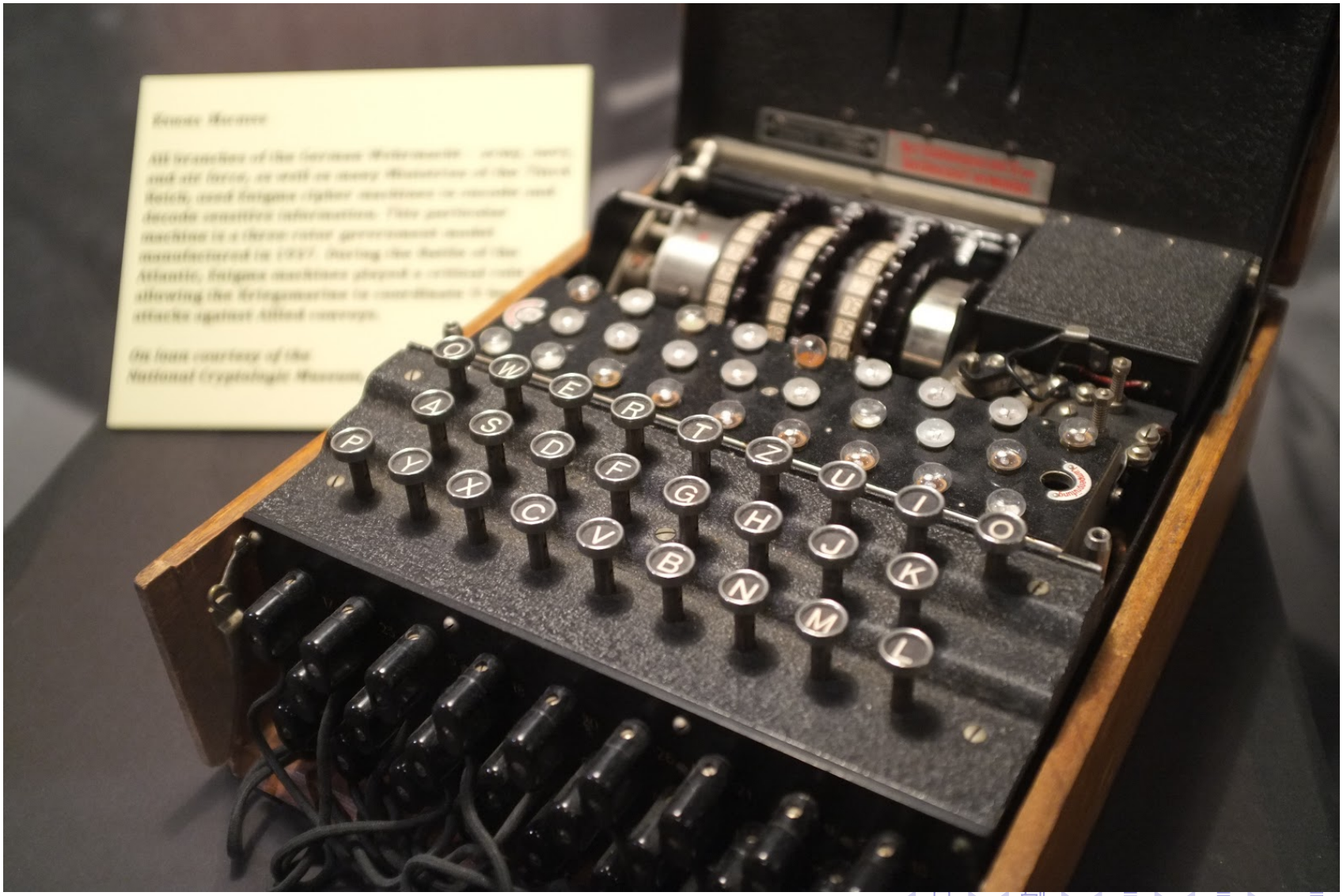
GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

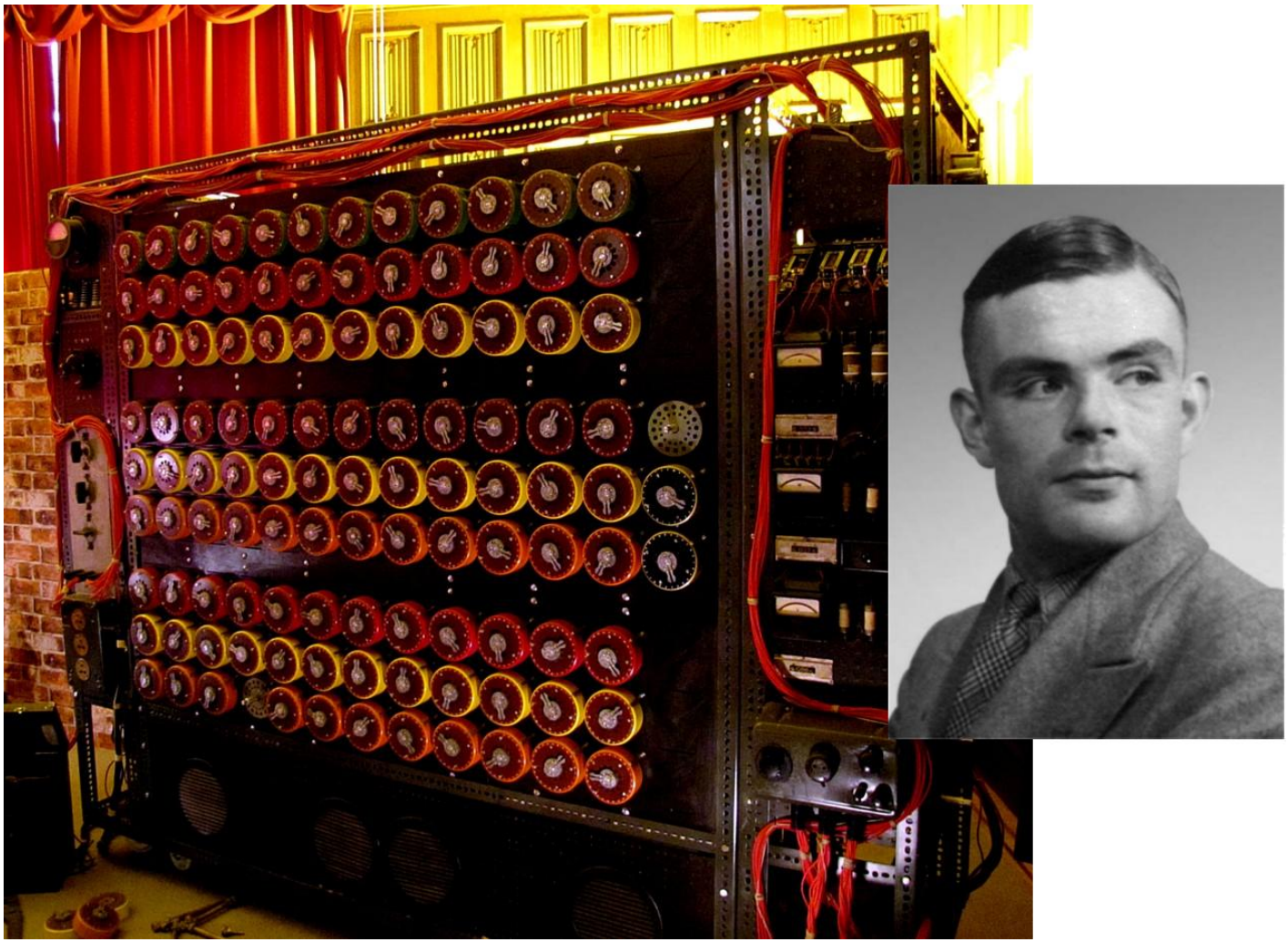
BEPNSTORFF.

Charge German Embassy.

The Enigma Machine



Alan Turing



Pearl Harbor

End of Historic Interlude

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust
- Impersonate you

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust
- Impersonate you
- Transfering your messages to someone else

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust
- Impersonate you
- Transfering your messages to someone else (STILL NAIVE!)

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust
- Impersonate you
- Transfering your messages to someone else (STILL NAIVE!)
- (KR) Steal your secret key

Adversarial Threat Models

What are you afraid of? What can your attacker do?

- Capture one encrypted message (YOU'RE EXTREMELY NAIVE!)
- Listen to all your communications (YOU'RE VERY NAIVE!)
- (CPA) Trick you into encrypting messages
- (CCA) Trick you into decrypting ciphertexts
- Induce errors in your devices
- Impersonate someone you trust
- Impersonate you
- Transfering your messages to someone else (STILL NAIVE!)
- (KR) Steal your secret key (STILL NAIVE BY THE WAY)

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

What do we expect from Cryptography

Musts:

1. Secrecy
2. Integrity
3. Authenticity

And then

- Advanced Threat Models
- Protocols
- *Flexibility*

UNDERSTOOD, JUST SHOW ME HOW IT'S DONE!

OK, but first...

UNDERSTOOD, JUST SHOW ME HOW IT'S DONE!

OK, but first...

Don't try this at home!

1.- Never Implement Your Own Cryptography

Practice works well in theory. Theory doesn't work well in practice.

2.- Complexity is your enemy

Research and Peer Review is paramount.

Don't try this at home!

1.- Never Implement Your Own Cryptography

Practice works well in theory. Theory doesn't work well in practice.

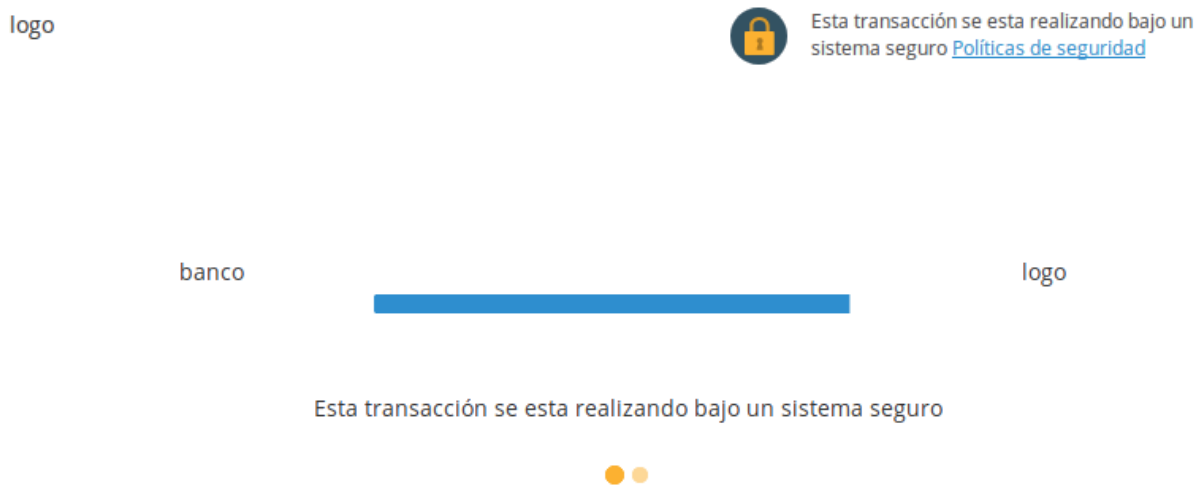
2.- Complexity is your enemy

Research and Peer Review is paramount.

Don't try this at home!

3.- Never Claim Your System Is Secure

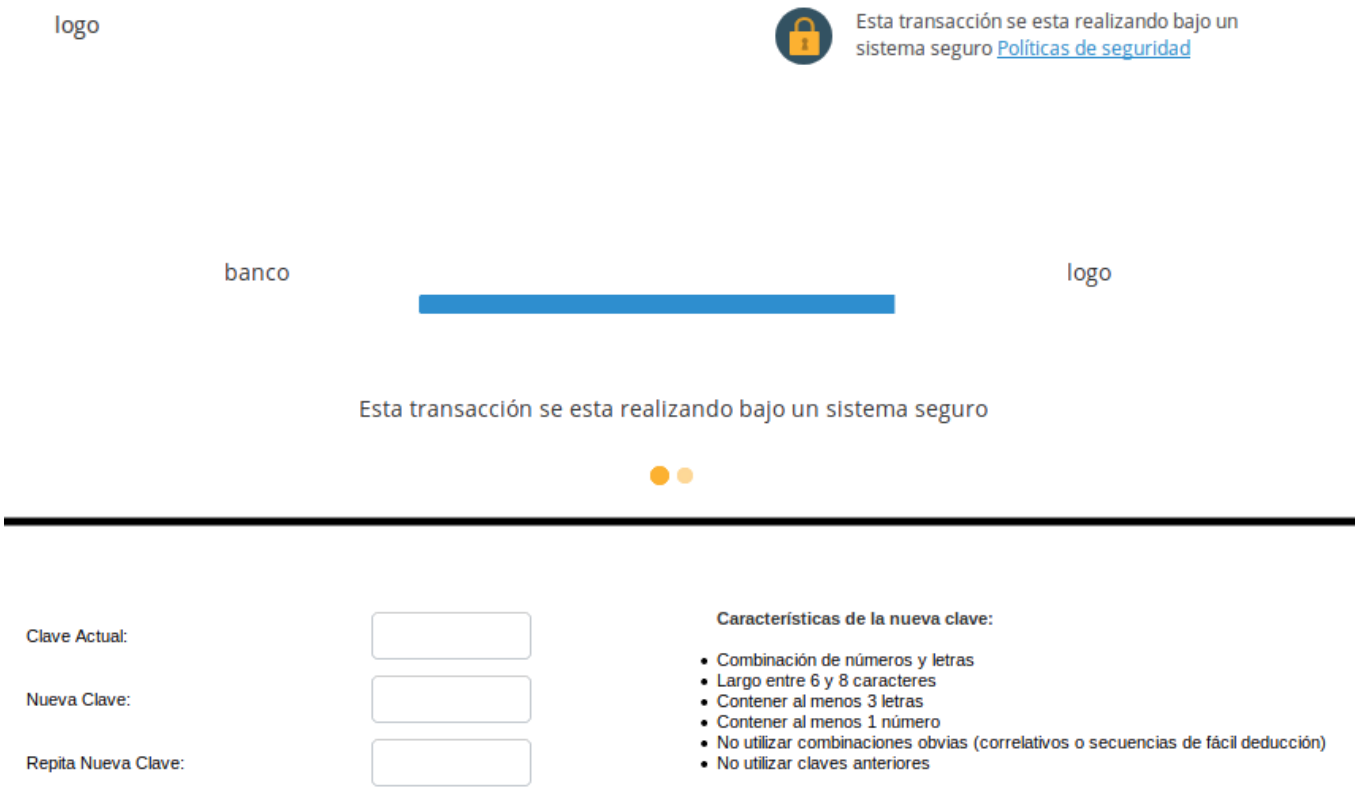
If you do, then your threat model is naïve



Don't try this at home!

3.- Never Claim Your System Is Secure

If you do, then your threat model is naïve



Probable vs. Provable

Let P be a mathematical problem. Let S be a cryptographic scheme and M a threat model.

Then S is **provably secure** under threat model M if any M-adversary that attacks S successfully can solve P.

Fantastic example:

- P = Riemann's Hypothesis
- S = Your email account
- M = Reading the text of your latest email

Probable vs. Provable

Let P be a mathematical problem. Let S be a cryptographic scheme and M a threat model.

Then S is **provably secure** under threat model M if any M-adversary that attacks S successfully can solve P.

Fantastic example:

- $P =$ Riemann's Hypothesis
- $S =$ Your email account
- $M =$ Reading the text of your latest email

Hall of fame problems in Hardness reductions

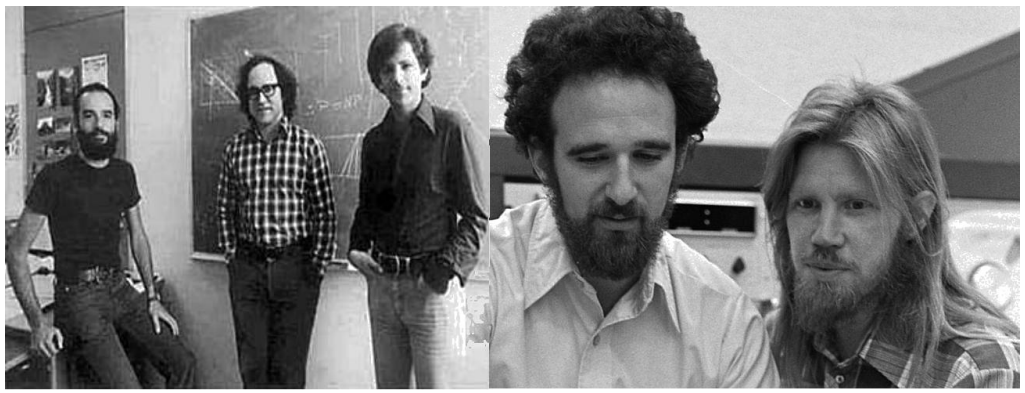
Integer Factorization Problem

Let p, q be two prime numbers. Guess p, q from $n = pq$.

Discrete Logarithm Problem

Let p be a prime number and $g \neq 0, 1$. Given g, p, b, guess x such that

$$g^x = b \bmod p.$$



But much, much more...

$$LWE \begin{cases} 3x_1 + 2x_2 - 4x_3 + \cdots + 3x_{1028} & \approx & 1 \\ -x_1 - 3x_2 + x_3 + \cdots - x_{1028} & \approx & -13 \\ 2x_1 + 2x_2 - 4x_3 + \cdots + 2x_{1028} & \approx & 0 \\ -4x_1 + x_2 - 3x_3 + \cdots + x_{1028} & \approx & 9 \\ \vdots & \vdots & \vdots \end{cases}$$

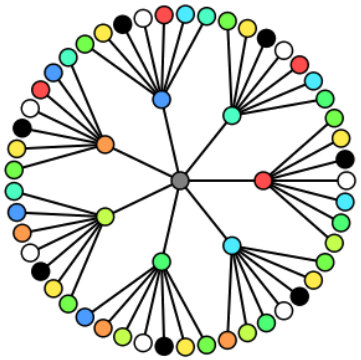
$$OV \begin{cases} x_1^2 + 2x_1x_2 - 4x_1x_3 + \cdots + 3x_{1028}^2 & = & 3 \\ 3x_1^2 - x_1x_2 + x_1x_3 + \cdots - x_{1028}^2 & = & 4 \\ -7x_1^2 - x_1x_2 + 2x_1x_3 + \cdots + 2x_{1028}^2 & = & 1 \\ 2x_1^2 + 2x_1x_2 + 3x_1x_3 + \cdots - 2x_{1028}^2 & = & 0 \\ \vdots & \vdots & \vdots \end{cases}$$

But much, much more...

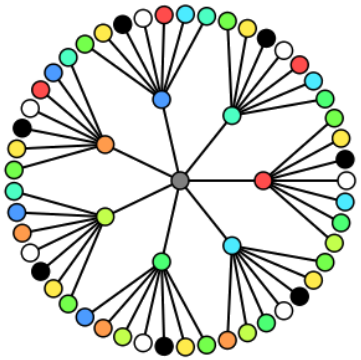
$$LWE \begin{cases} 3x_1 + 2x_2 - 4x_3 + \cdots + 3x_{1028} & \approx & 1 \\ -x_1 - 3x_2 + x_3 + \cdots - x_{1028} & \approx & -13 \\ 2x_1 + 2x_2 - 4x_3 + \cdots + 2x_{1028} & \approx & 0 \\ -4x_1 + x_2 - 3x_3 + \cdots + x_{1028} & \approx & 9 \\ \vdots & \vdots & \vdots \end{cases}$$

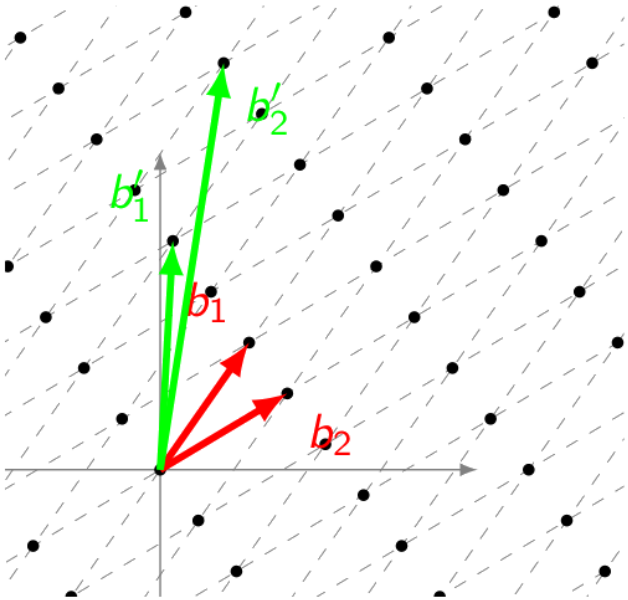
$$OV \begin{cases} x_1^2 + 2x_1x_2 - 4x_1x_3 + \cdots + 3x_{1028}^2 & = & 3 \\ 3x_1^2 - x_1x_2 + x_1x_3 + \cdots - x_{1028}^2 & = & 4 \\ -7x_1^2 - x_1x_2 + 2x_1x_3 + \cdots + 2x_{1028}^2 & = & 1 \\ 2x_1^2 + 2x_1x_2 + 3x_1x_3 + \cdots - 2x_{1028}^2 & = & 0 \\ \vdots & \vdots & \vdots \end{cases}$$

But much, much more...

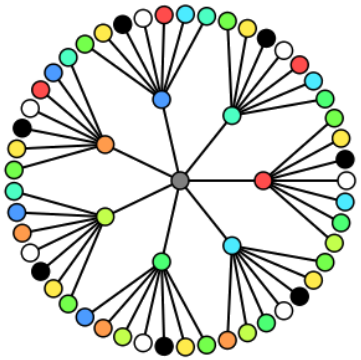


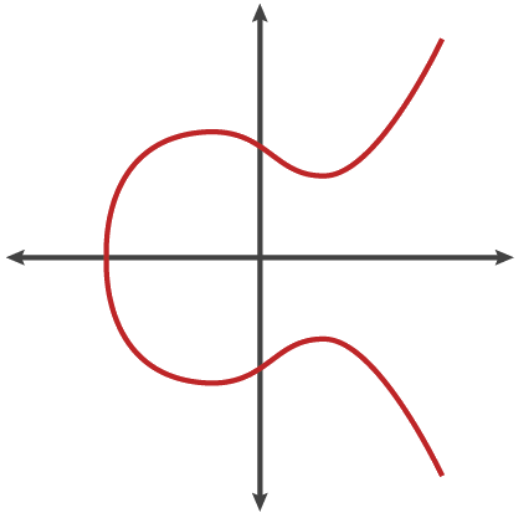
But much, much more...

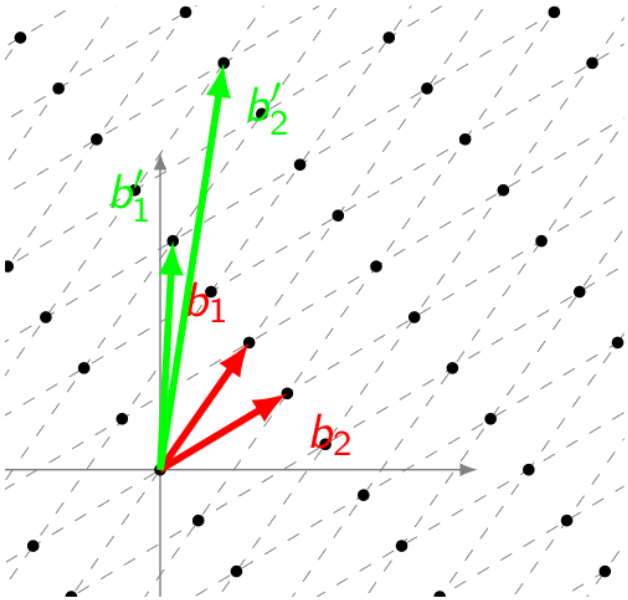




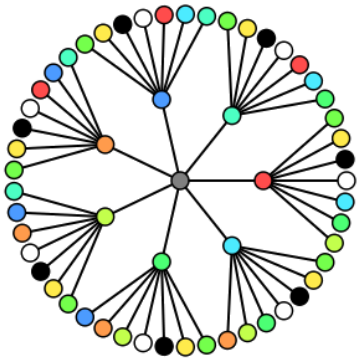
But much, much more...

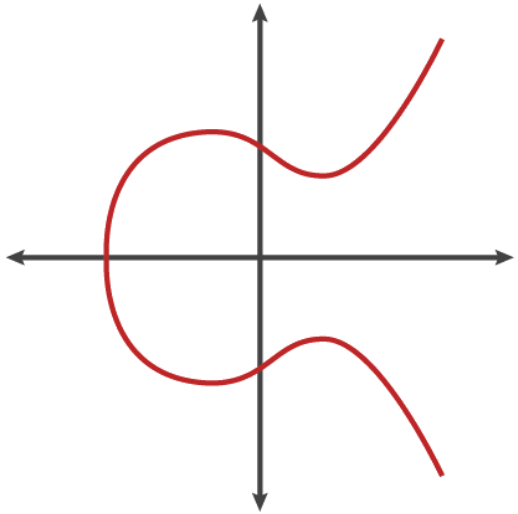


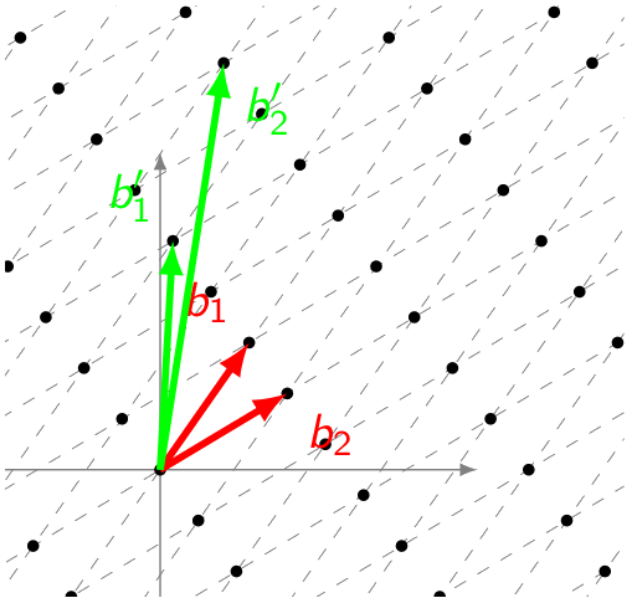


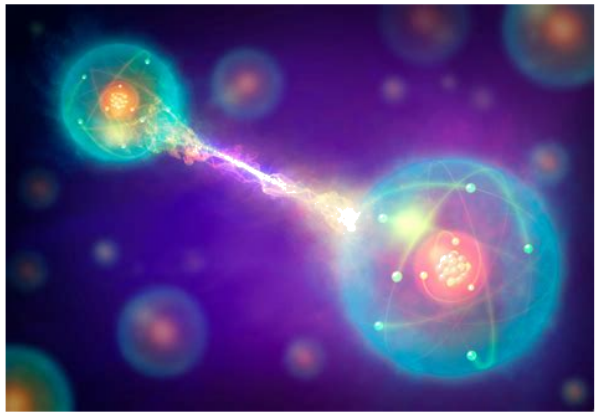


But much, much more...









$$\langle \psi | \phi \rangle$$

New Protocols

Secure Multiparty Computation

Alice has x, Bob has y, compute $f(x, y)$ without sharing x, y.
(Example: Yao's Millionaire Problem)

Fully Homomorphic Encryption

Perform operations over encrypted data

Deniable Encryption

Fake-bottom drawers

Whitebox Cryptography

Perfect Playstation

New Protocols

Secure Multiparty Computation

Alice has x, Bob has y, compute $f(x, y)$ without sharing x, y.
(Example: Yao's Millionaire Problem)

Fully Homomorphic Encryption

Perform operations over encrypted data

Deniable Encryption

Fake-bottom drawers

Whitebox Cryptography

Perfect Playstation

New Protocols

Secure Multiparty Computation

Alice has x, Bob has y, compute $f(x, y)$ without sharing x, y.
(Example: Yao's Millionaire Problem)

Fully Homomorphic Encryption

Perform operations over encrypted data

Deniable Encryption

Fake-bottom drawers

Whitebox Cryptography

Perfect Playstation

New Protocols

Secure Multiparty Computation

Alice has x, Bob has y, compute $f(x, y)$ without sharing x, y.
(Example: Yao's Millionaire Problem)

Fully Homomorphic Encryption

Perform operations over encrypted data

Deniable Encryption

Fake-bottom drawers

Whitebox Cryptography

Perfect Playstation

Real World Problems

Cryptography vs. Software and Hardware

Side channel attacks

Cryptography vs. Law

Non-repudiability

Cryptography vs. Industry

Efficiency, flexibility

Real World Problems

Cryptography vs. Software and Hardware

Side channel attacks

Cryptography vs. Law

Non-repudiability

Cryptography vs. Industry

Efficiency, flexibility

Real World Problems

Cryptography vs. Software and Hardware

Side channel attacks

Cryptography vs. Law

Non-repudiability

Cryptography vs. Industry

Efficiency, flexibility

Why study cryptography

1.- Because my data will outlive me
Privacy IS possible.

2.- Spectacular application of mathematics
Exciting Research/Industry jobs available.

3.- Because Latin America needs it more than ever

Why study cryptography

1.- Because my data will outlive me
Privacy IS possible.

2.- Spectacular application of mathematics
Exciting Research/Industry jobs available.

3.- Because Latin America needs it more than ever

Why study cryptography

1.- Because my data will outlive me
Privacy IS possible.

2.- Spectacular application of mathematics
Exciting Research/Industry jobs available.

3.- Because Latin America needs it more than ever

Thank you!