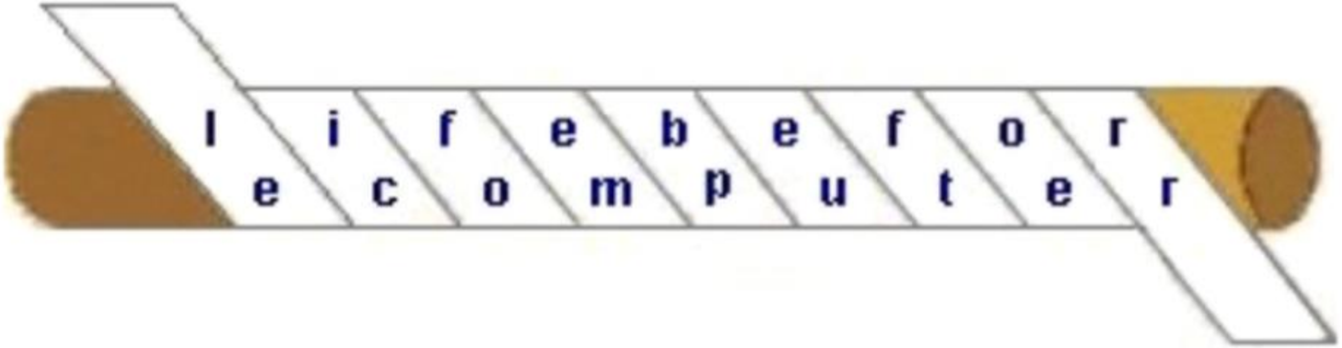

CRYPTOGRAPHY

Some examples

Scitala lacedemone (900 ac)



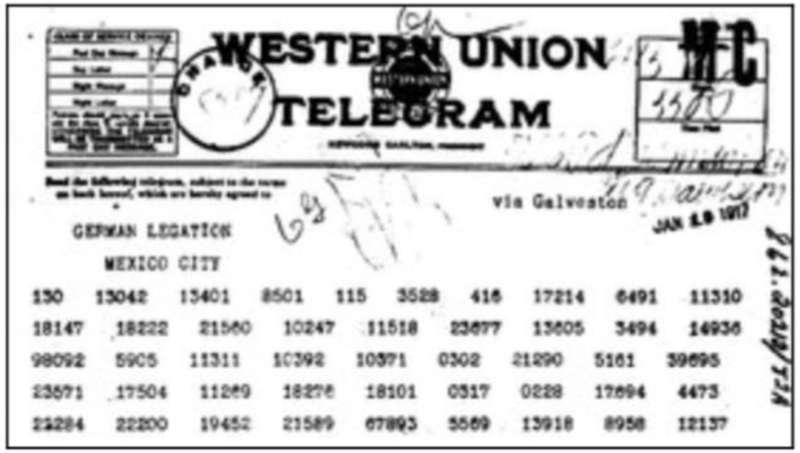
The Julius Caesar code

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
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

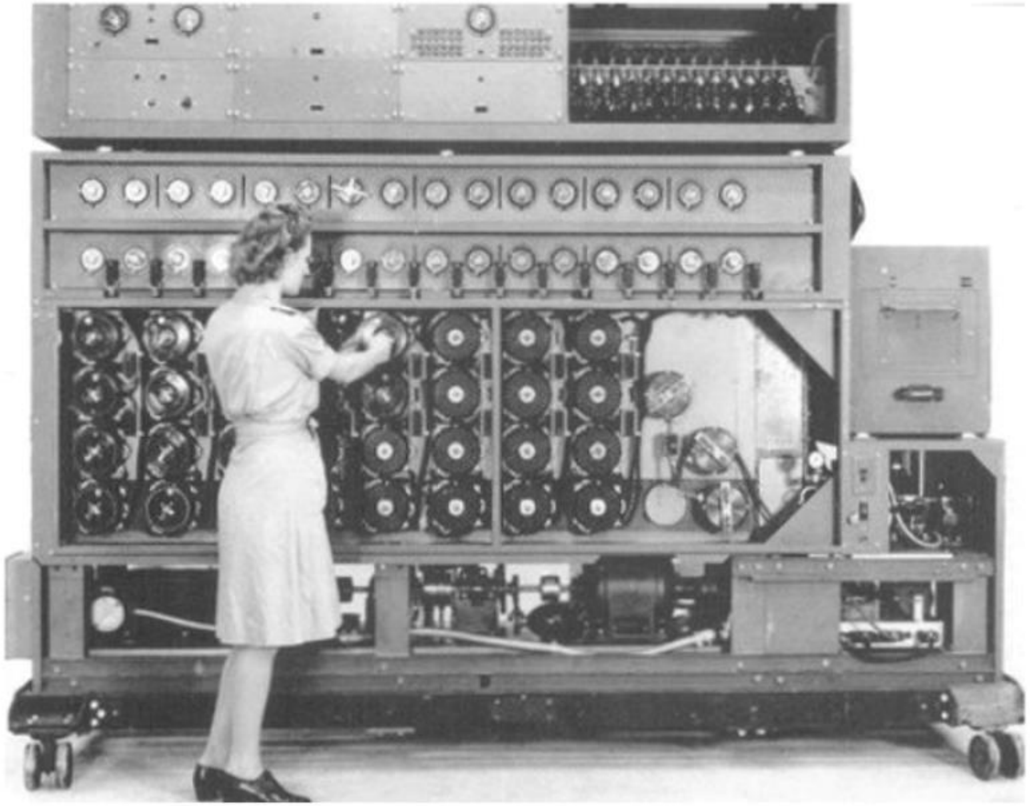
Example: BELUGKQDJKCZXOIYSI

Features:

- both who sends and who receives must know the "key"
- if someone intercepts the "key", he/she is able to decrypt the messages



ENIGMA (II World World War)
German army coding machine:
with only 3 disks there are
10^{15} combinations



STATION X (Bletchley Park, UK):
January 1945, more than 10,000 people whose work was entirely devoted to decoding German messages; mathematicians team was headed by Alan Turing

```
eb 04 af c2 bf a3 81 ec  00 01 00 00 31 c9 88 0c
0c fe c1 75 f9 31 c0 ba  ef be ad de 02 04 0c 00
d0 c1 ca 08 8a 1c 0c 8a  3c 04 88 1c 04 88 3c 0c
fe c1 75 e8 e9 5c 00 00  00 89 e3 81 c3 04 00 00
00 5c 58 3d 41 41 41 41  75 43 58 3d 42 42 42 42
75 3b 5a 89 d1 89 e6 89  df 29 cf f3 a4 89 de 89
d1 89 df 29 cf 31 c0 31  db 31 d2 fe c0 02 1c 06
8a 14 06 8a 34 1e 88 34  06 88 14 1e 00 f2 30 f6
8a 1c 16 8a 17 30 da 88  17 47 49 75 de 31 db 89
d8 fe c0 cd 80 90 90 e8  9d ff ff ff 41 41 41 41
```

This is the code to be solved to become an analyst at English C.G.H.Q. (Communication HeadQuartes). Do you want to try?

If you can solve it, on the screen: it's hard work for motivated people, but the salary is very high!

PUBLIC KEY CRYPTOGRAPHY:

- asymmetric system consisting of two different keys, a public one for encryption and a secret one for deciphering
- he public key is an integer of the type $n = p * q$, where p and q are two prime numbers
- the secret key is linked to the value of one of the two factors

The security of the protocol is based on the fact that to find the secret key it is necessary to know the two factors p and q: this requires a very long time for a computer.

516 bit key = 6 weeks with office computer network

PUBLIC KEY CRYPTOGRAPHY:

- asymmetric system consisting of two different keys, a public one for encryption and a secret one for deciphering
- he public key is an integer of the type $n = p * q$, where p and q are two prime numbers
- the secret key is linked to the value of one of the two factors

The security of the protocol is based on the fact that to find the secret key it is necessary to know the two factors p and q: this requires a very long time for a computer.

RSA-768 =
1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202021
99786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602
221240479274737794080665351419597459856902143413

typical computer: 10^{115} elementary instructions, CPU 10 billion operations per second -> 10^{97} years dedicated computer network: factored in 2009 after two years of calculation a quantum computer? a few days / hour!

If we had a quantum computer, WOULD OUR DATA BE IN DANGER?

February 2016: National Security Agency USA launched an alarm, inviting to use more robust keys.

YES

but ...

quantum physics also provides a new protocol to make our transmissions secure

CRYPTO 1984: Advances in Cryptology pp 475-480 | Cite as

An Update on Quantum Cryptography

Authors Authors and affiliations

Charles H. Bennett, Gilles Brassard

Both Alice and Bob can make measurements both along X and along Z, randomly and independently of each other, on the same qubit.


Bob
1
0
1
0
Alice
(source)
|↓⟩ In vacuum
Z
X
Random orientations
Fixed orientations
Z
X
Introduction
Display controls
Show key generation
Show key bits
Show total errors
Clear measurements
Alice
Basis Value
Eve
Basis Outcome
Bob
Basis Outcome
Alice and Bob
Same bases?
Key
Z 0 Z 0 YES 0
Z 0 Z 0 YES 0
Z 0 Z 0 YES 0
Z 0 Z 0 YES 0
Z 1 Z 1 YES 1
Z 0 Z 0 YES 0


Bob
1
0
1
0
Alice
(source)
|↑⟩ In vacuum
Z
X
Random orientations
Fixed orientations
Z
X
Introduction
Display controls
Show key generation
Show key bits
Show total errors
Clear measurements
Alice
Basis Value
Eve
Basis Outcome
Bob
Basis Outcome
Alice and Bob
Same bases?
Key
Z 1 X 1 NO
Z 0 X 0 NO
Z 0 X 1 NO
Z 0 X 0 NO
Z 0 X 1 NO
Z 1 X 1 NO

Display controls

- [x] Show key generation
- [ ] Show key bits
- [ ] Show total errors

Clear measurements

Alice Basis	Alice Value	Eve Basis	Eve Outcome	Bob Basis	Bob Outcome	Alice and Bob Same bases?	Key
X	0			Z	1	NO	
Z	1			Z	1	YES	1
Z	0			Z	0	YES	0
X	0			X	0	YES	0
Z	1			Z	1	YES	1
Z	1			Z	1	YES	1

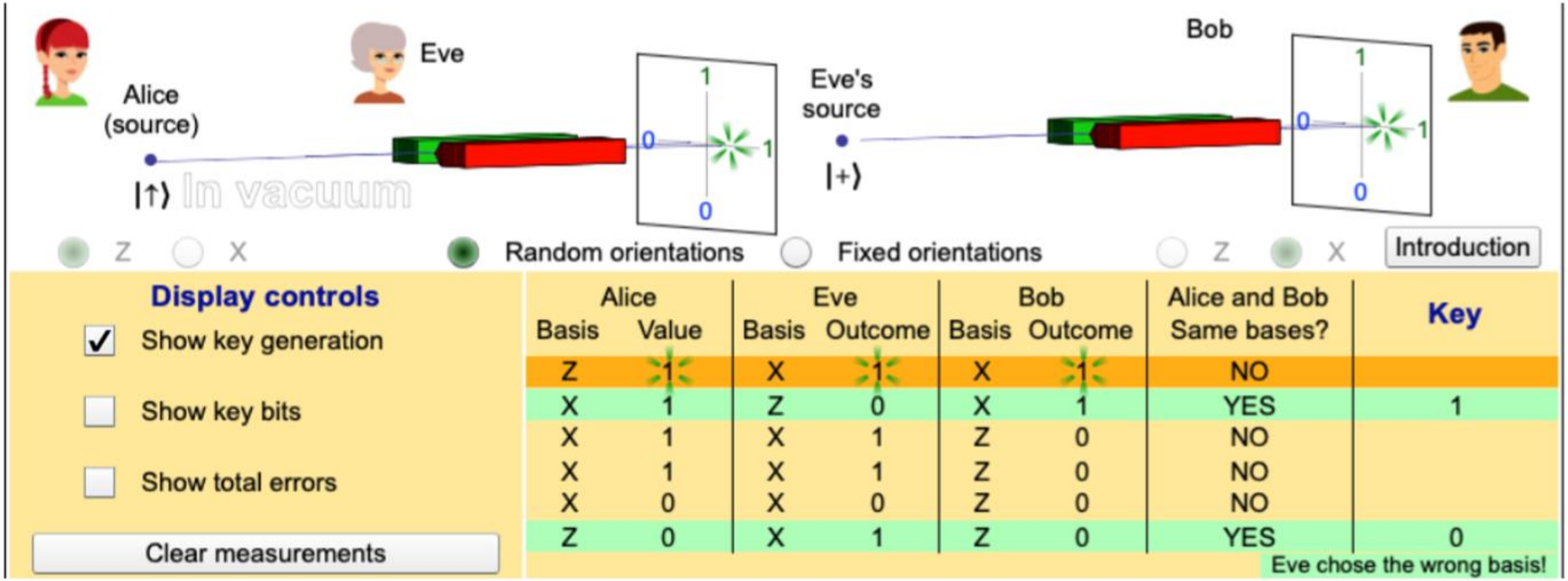
Display controls

- [x] Show key generation
- [ ] Show key bits
- [ ] Show total errors

Clear measurements

Alice Basis	Alice Value	Eve Basis	Eve Outcome	Bob Basis	Bob Outcome	Alice and Bob Same bases?	Key
Z	1			Z	1	YES	1
Z	0			Z	0	YES	0
X	1			X	1	YES	1
X	0			Z	1	NO	
Z	0			X	0	NO	
X	1			X	1	YES	1

KEY GENERATION (SECRET)



PRESENCE OF EVE INTERCEPTING, Alice and Bob can see it by comparing (publicly) a subset of their data.

https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/cryptography-bb84/Quantum_Cryptography.html


http://toutestquantique.fr/
https://www.st-andrews.ac.uk/physics/quvis/