👀Encryption Overview

Huiyue Bai
Situ Feng

Table of Contents 📕


LEFT
EXIT 12
Afraid of Math
Expert in Math & Encryption
You
imgflip.com

What is Encryption ?

- The process of ***encoding*** information
- PlainText + Encryption = CipherText
- CipherText + Decryption = PlainText

When did encryption become a thing ?

1900 B.C. -> 700 B.C. -> The Middle Ages -> 1976

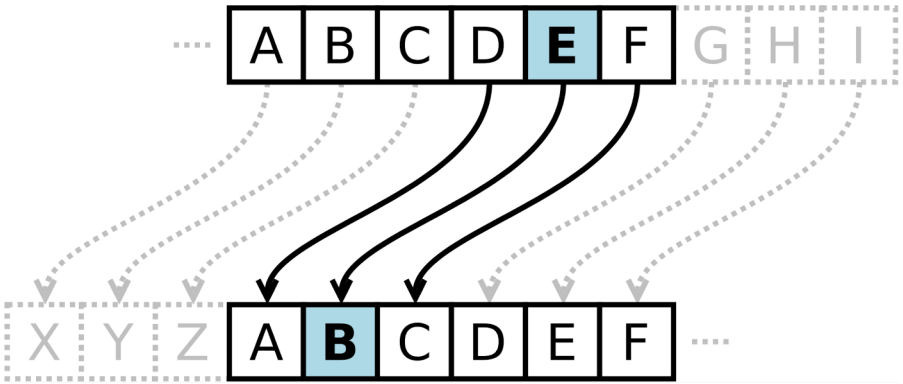
1900 B.C. an Egyptian scribe used nonstandard hieroglyphs to hide the meaning of an inscription

When did encryption become a thing ?

1900 B.C. -> ***700 B.C.*** -> The Middle Ages -> 1976

700 B.C. - Caesar Shift Cipher

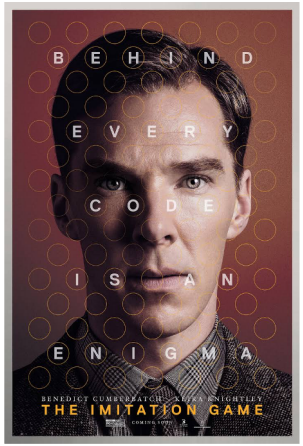
HELLO WORLD -> EBIIL TLOIA



When did encryption become a thing ?

1900 B.C. -> 700 B.C. -> ***1940s*** -> 1976

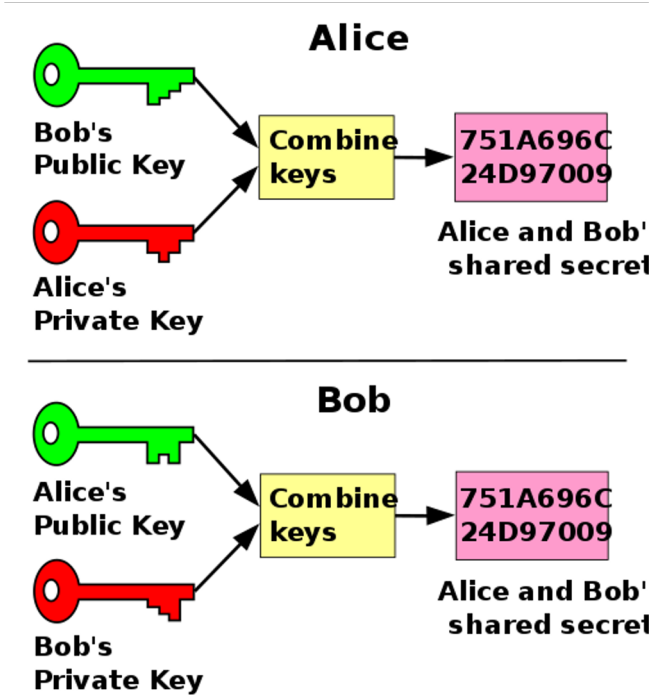
1940s - Enigma Machine & Turing Machine (*Ui f !Jh jubjpo!Hbn f **)



When did encryption become a thing ?

1900 B.C. -> 700 B.C. -> The Middle Ages -> ***1976***

1976 - “New Direction in Cryptography” by Whitfield Diffie and Martin Hellman



Why do we need encryption anyway ?

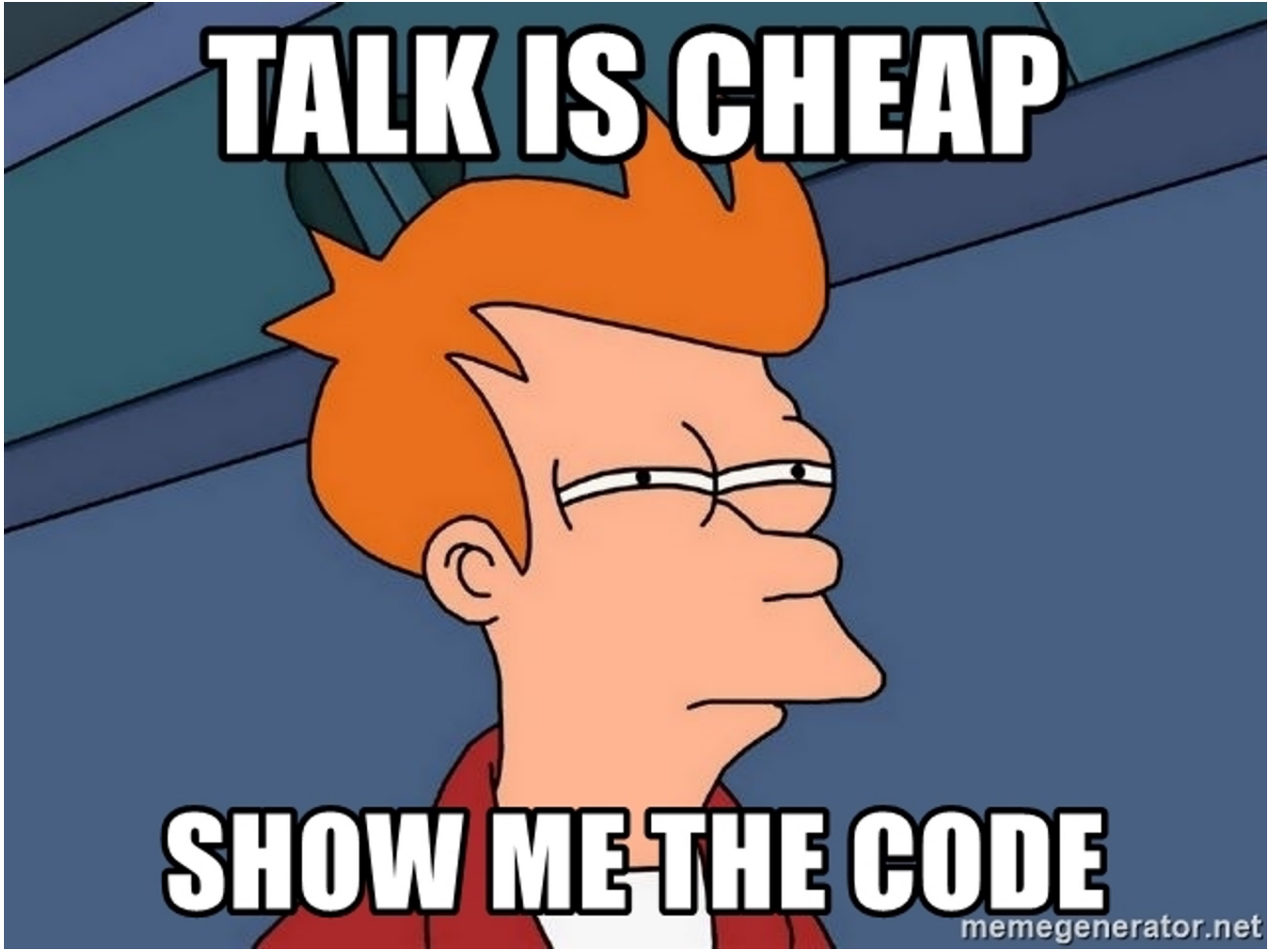
What is the motivation behind it?

- Need privacy

Why do we need encryption anyway ?

What is the motivation behind it?

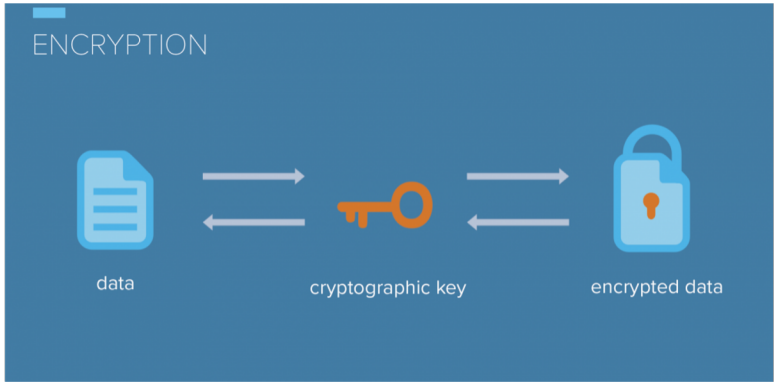
- Laws
  - the Payment Card Industry Data Security Standard (PCIDSS) requires merchants to encrypt customers' payment card data


TALK IS CHEAP
SHOW ME THE CODE
memegenerator.net

How does encryption work ?

Encryption uses ***algorithms*** to scramble the information in a way such that only certain people can read/understand it.

In other words, it requires ***ciphers*** to get the job done!



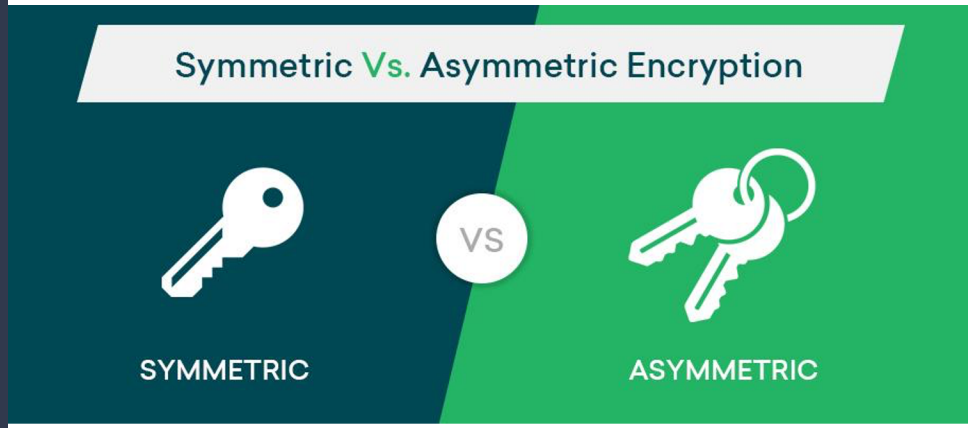
What are ciphers ?

- An algorithm for performing encryption/decryption
- A series of well-defined steps that can be followed as a procedure

What are ciphers ?

What ciphers are mostly-used?

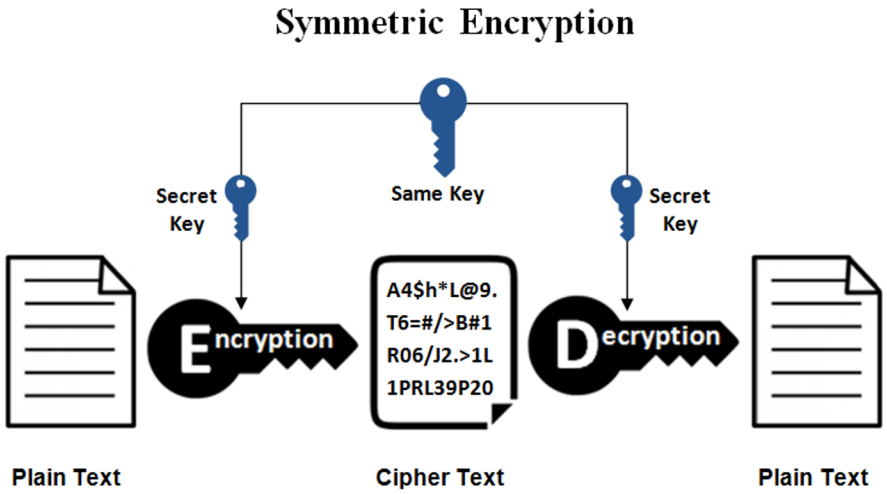
- Symmetric cipher
  - ***Same*** key for encryption/decryption
- Asymmetric cipher
  - ***Different*** keys for encryption/decryption



What are ciphers ?

What ciphers are mostly-used?

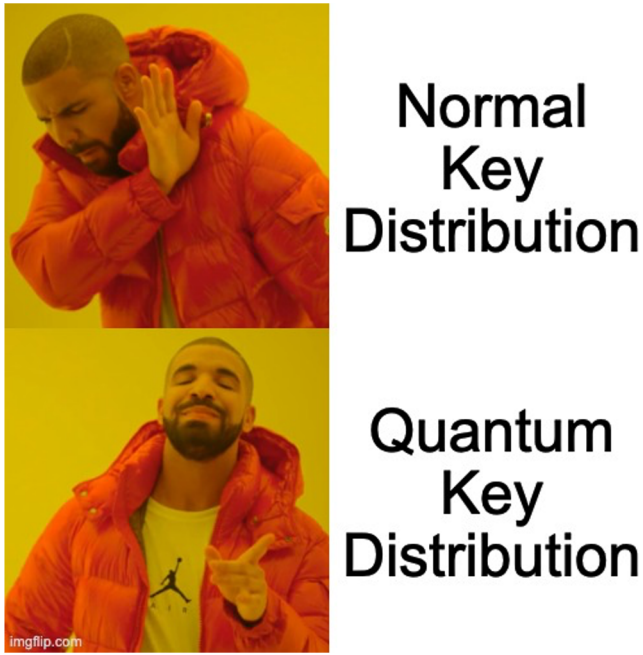
- Symmetric ciphers
  - AES (Advanced Encryption Standard)
  - https://www.youtube.com/watch?v=O4xNJsjtN6E&t=393s



What are ciphers ?

What ciphers are mostly-used?

- Symmetric ciphers
  - Quantum key distribution (QKD)



What are ciphers ?

What ciphers are mostly-used?

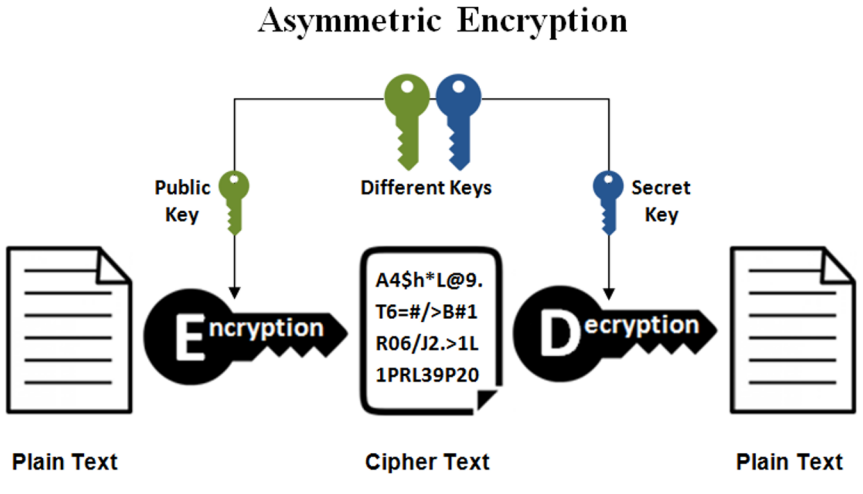
- Quantum key distribution (QKD)
  - relies on quantum mechanics

- Traditional Public-Key Cryptography
  - relies on computational difficulty on certain mathematical functions
  - i.e. factorize a large integer

What are ciphers ?

What ciphers are mostly-used?

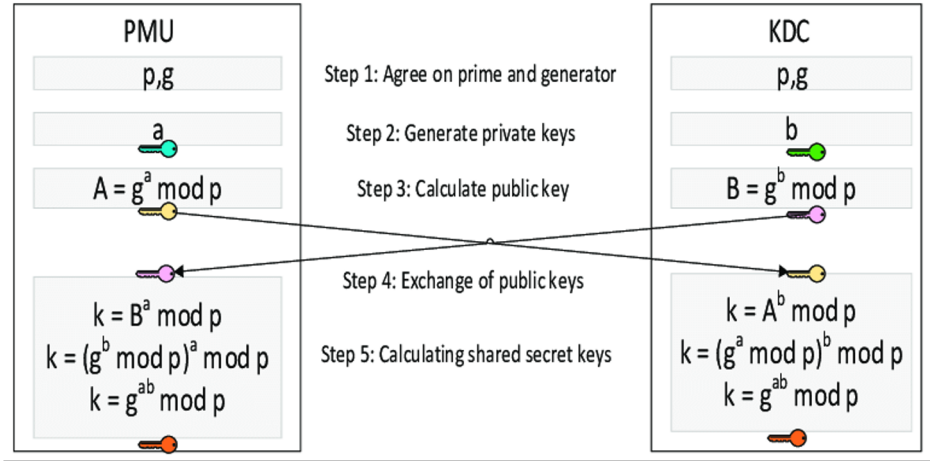
- Asymmetric cipher
  - RSA (Rivest-Shamir-Adleman)



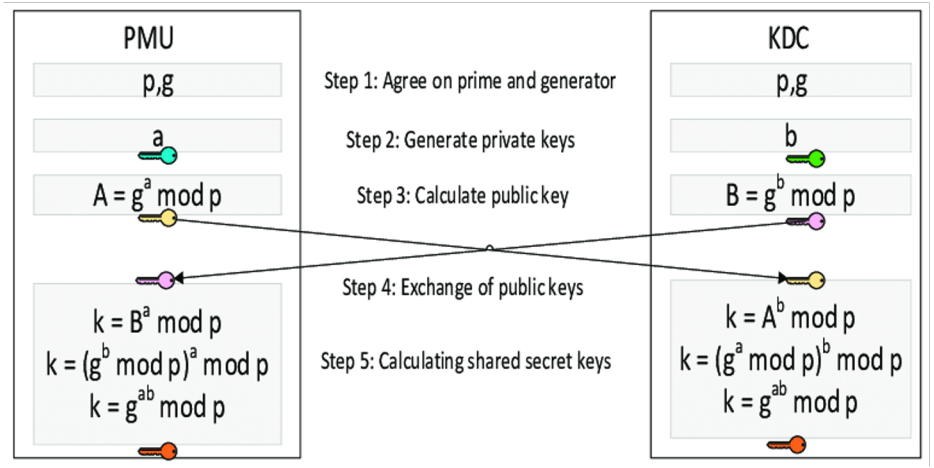
What are ciphers ?

What ciphers are mostly-used?

- Asymmetric cipher
  - Diffie-Hellman key exchange



Diffie-Hellman Key Exchange Example



p = 23, g = 9

Alice: a = 4 *Bob: b = 3*

Alice: $A = g^a \bmod p = 9^4 \bmod 23 = 6$

Bob: $B = g^b \bmod p = 9^3 \bmod 23 = 16$

Alice: $k = B^a \bmod p = 16^4 \bmod 23 = 9$

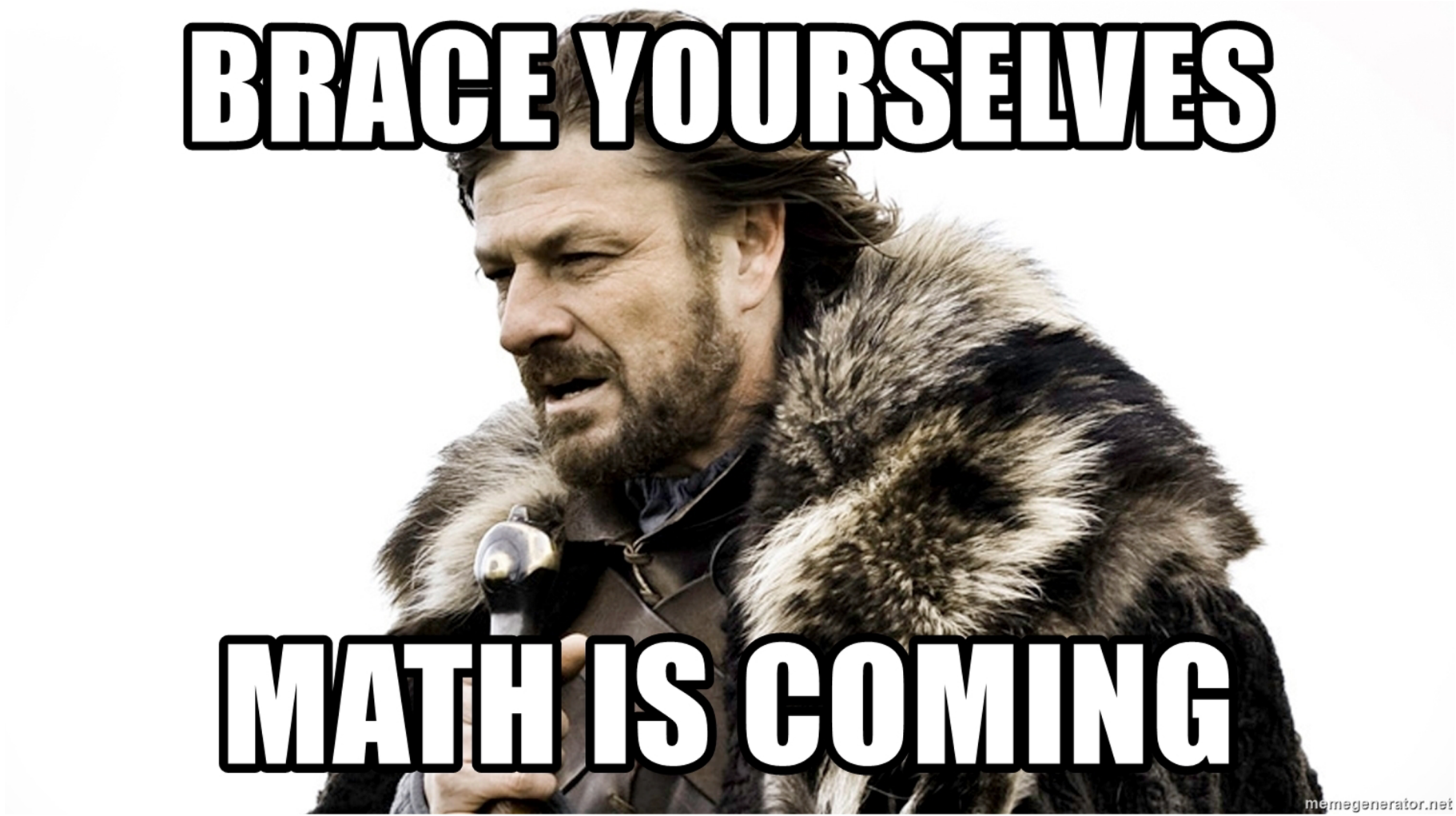
Bob: $k = A^b \bmod p = 6^3 \bmod 23 = 9$

What are ciphers ?

What ciphers are mostly-used?

- Asymmetric cipher
  - ***Elliptic curve*** cryptography (ECC)
  - a.k.a. “better” RSA

  Wait, what is a elliptic curve?


BRACE YOURSELVES
MATH IS COMING
memegenerator.net

What are ciphers ?

What ciphers are mostly-used?

- In mathematics ***elliptic curves*** are plane algebraic curves, consisting of all points {x, y}, described by the equation:

$$A x^3 + B x^2 y + C x y^2 + D y^3 + E x^2 + F x y + G y^2 + H x + I y + J = 0,$$

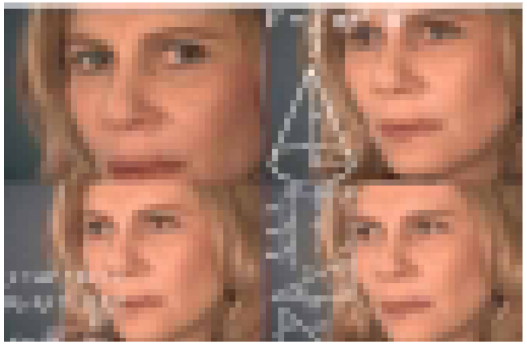
What are ciphers ?

What ciphers are mostly-used?

- Cryptography uses elliptic curves in a ***simplified*** form (Weierstrass form), which is defined as:

$$y^2 = x^3 + ax + b$$

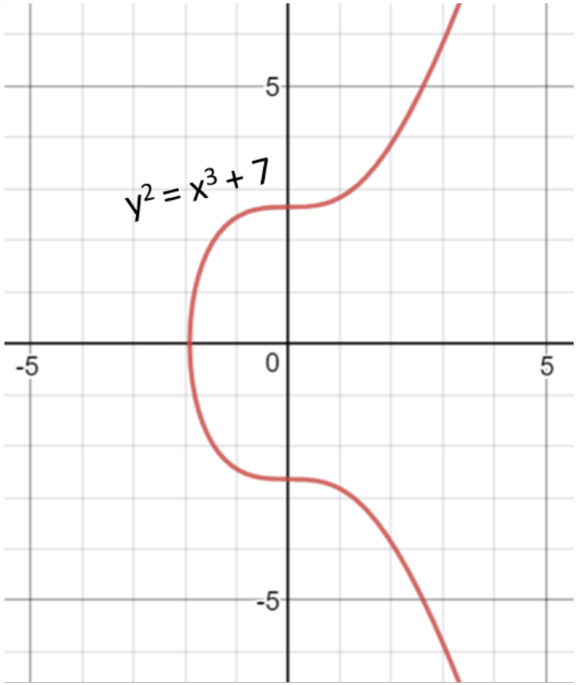
where ***a, b*** are parameters



What are ciphers ?

What ciphers are mostly-used?

- The famous NIST curve ***secp256k1*** (used in Bitcoin) is based on the elliptic curve with ***a = 0, b = 7***



Note: Different curves provide different level of ***security***, different ***performance***, and different ***key length***

What are ciphers ?

What ciphers are mostly-used?

- ***Elliptic Curve Cryptography*** (ECC)
  - uses ***elliptic curves*** over the finite field
  - the field is a square matrix of $p \times p$
  - p is prime and $p > 3$
  - points are ***integer*** coordinates {x,y}

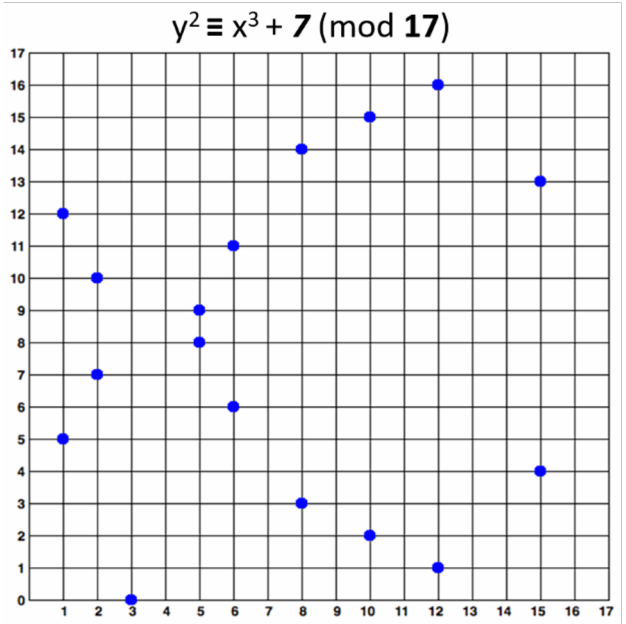
What are ciphers ?

What ciphers are mostly-used?

- ***Elliptic Curve Cryptography*** (ECC)
  - uses ***elliptic curves*** over the finite field
  - the field is a square matrix of $p \times p$
  - p is prime and $p > 3$
  - points are ***integer*** coordinates {x,y}

    $\Rightarrow 0 \leq x, y < p$

    e.g. the Bitcoin curve



Elliptic Curve Cryptography

- Two EC points can be ***added*** and result in another point. a.k.a. ***EC point addition***

  G: the generator point

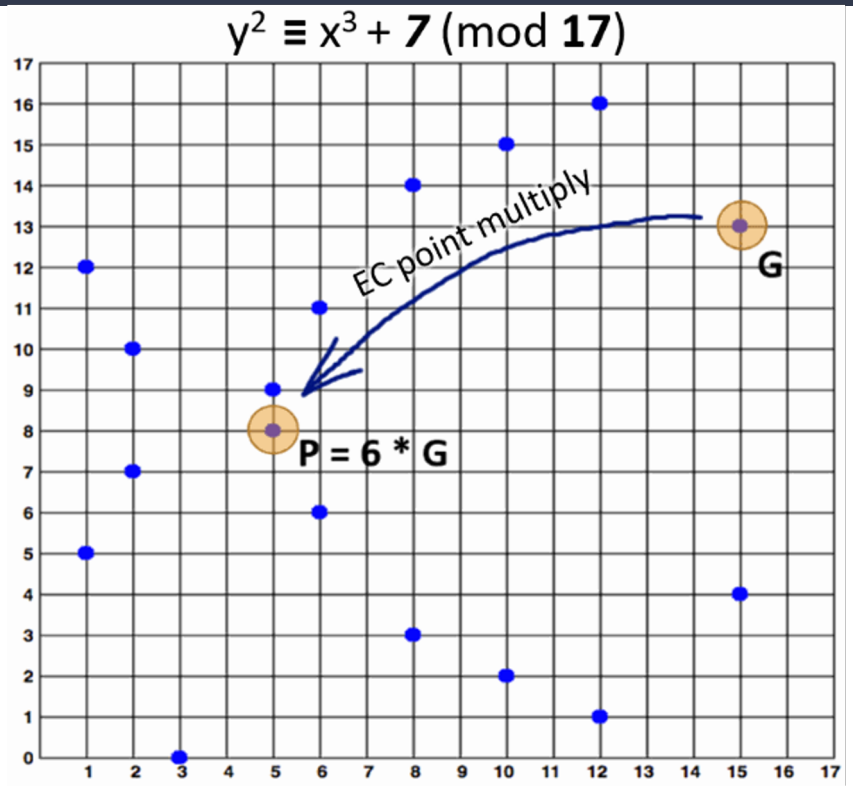
  k: an integer (private key)

  P: obtained EC point (public key)

  P = k * G

e.g.

G = {15, 13}, k = 6
P = k * G = 6 * {15, 13} = {5, 8}



Elliptic Curve Discrete Logarithm Problem

- By given elliptic curve over finite field $\mathbb{F}_p$ and generator point ***G*** on the curve and point ***P*** on the curve, find the integer ***k*** (if it exists), such that ***P = k * G***

- Recall:
  P: public key
  k: private key

What are ciphers ?

What ciphers are mostly-used?

- ***Elliptic Curve Cryptography*** (ECC)
  - ***private*** keys are integers in the range of the curve's field size (normally 256-bit)
  - e.g. hex encoded, 32 bytes, 64 hex digits

```
0x51897b64e85c3f714bba707e867914295a1377a7
463a9dae8ea6a8b914246319
```

- Don't panic, it's as simple as securely generating a random integer in certain range (i.e. very fast)

What are ciphers ?

What ciphers are mostly-used?

- ***Elliptic Curve Cryptography*** (ECC)
  - ***public*** keys are ***EC points*** (i.e. pairs of integer coordinates on the curve)
  - ***EC points*** can be compressed to just one coordinate + 1 bit (odd or even)
  - e.g. encode the ***y*** coordinate as prefix ***02*** or ***03***

```
0x02f54ba86dc1ccb5bed0224d23f01ed87e4a443c47fc690d7797a13d41d2340e1a
```

What are ciphers ?

What ciphers are mostly-used?

- ***Elliptic Curve Cryptography*** (ECC)
  - because it uses smaller keys than RSA for the same level of security
  - fast key generation!
  - fast key agreement!

50%

You have made it halfway!

Recap:

- Introduction to Encryption 👀
- History of Encryption 🗞️
- How does Encryption work 😲
- Examples of Encryption 🐾

We have covered

- Advanced Encryption Standard (AES)
- Quantum Key Distribution (QKD)
- Rivest-Shamir-Adleman (RSA)
- Diffie-Hellman Key Exchange
- Elliptic Curve Cryptography (ECC)


YOU MADE IT!
I'M IMPRESSED!
memegenerator.net

Why homomorphic encryption ?

Sensitive data (like medical data) needs computation/analysis

↓

They cannot give be given to the third party for calculation directly

↓

Homomorphic encryption can help!

What is Homomorphic Encryption ?

- A form of encryption that permits users to perform computations on its encrypted data ***without*** first decrypting it

Homomorphic Encryption

- Partially homomorphic encryption
  - either additively homomorphic or multiplicatively homomorphic

Homomorphic Encryption

- Somewhat homomorphic encryption
  - capable of doing both addition and multiplication to the original plaintexts but its capability is heavily limited

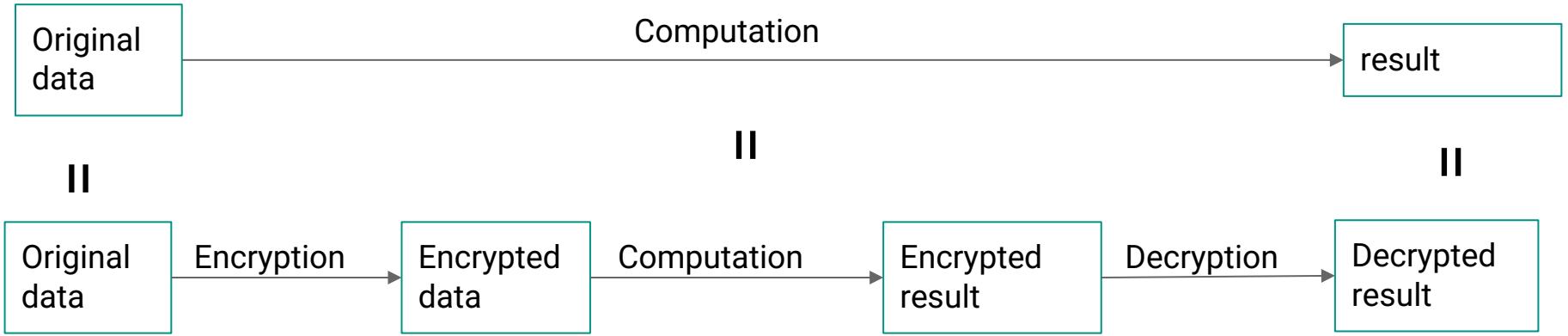
Homomorphic Encryption

- Fully homomorphic encryption
  - can do arbitrary computation to the plaintexts by manipulating the ciphertexts

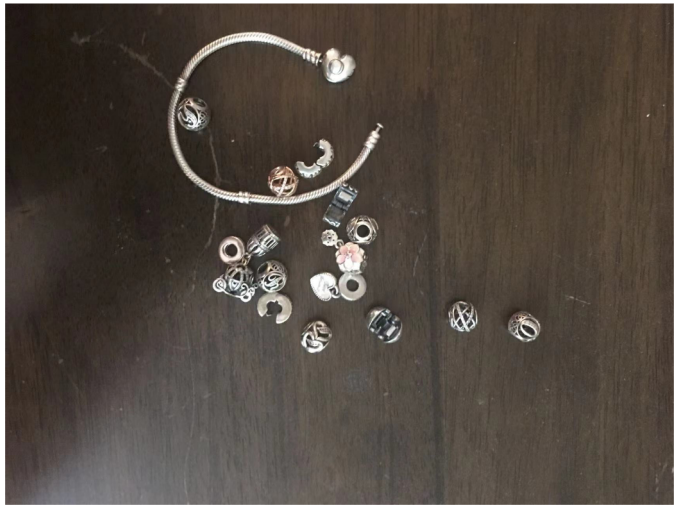
Fully Homomorphic Encryption

- Doctor Craig Gentry
  - constructed the first Fully Homomorphic Encryption scheme
    - Introduced bootstrapping

Homomorphic encryption



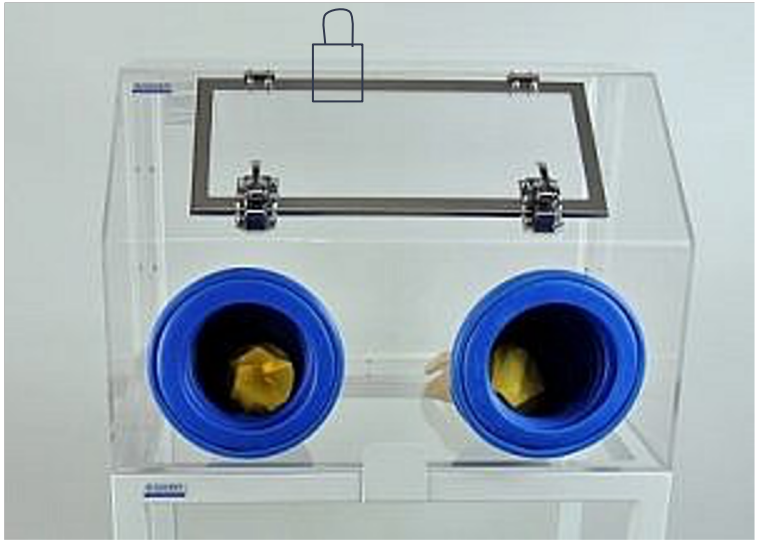
Alice’s Jewelry store



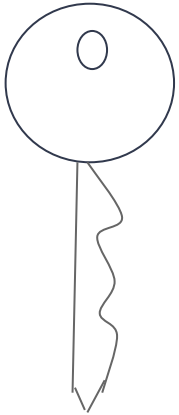
original

Finished item

Alice and gloveboxes



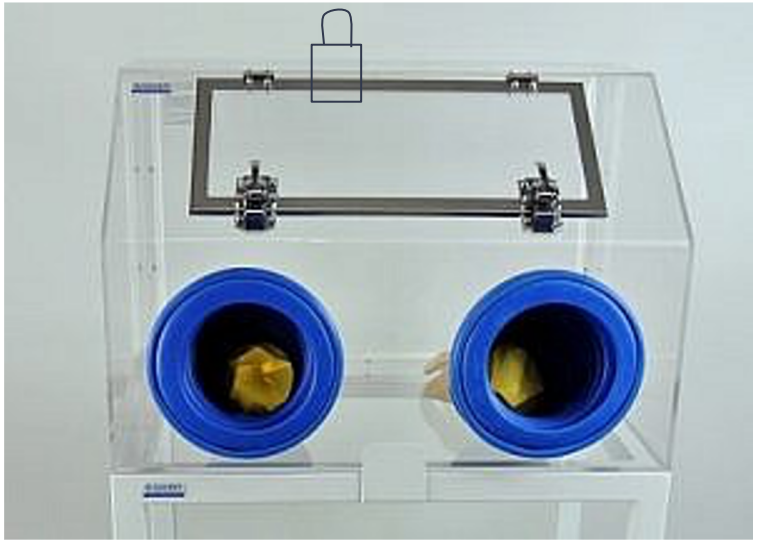
worker



Alice

The glove box

=

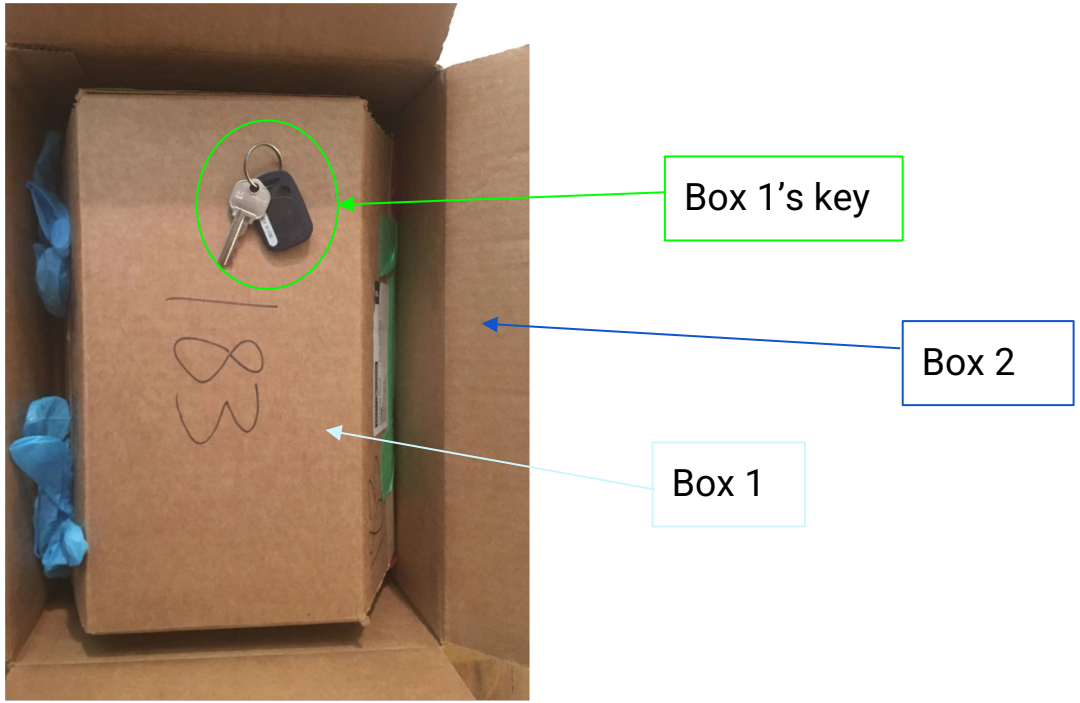


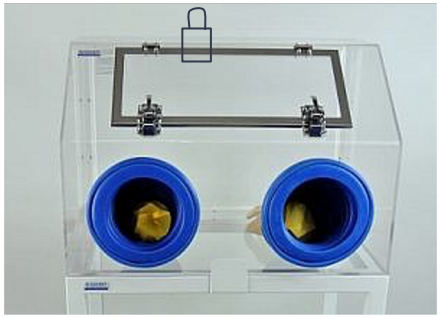
Worker is working on it.

Defective gloves

Need to change every
5 min

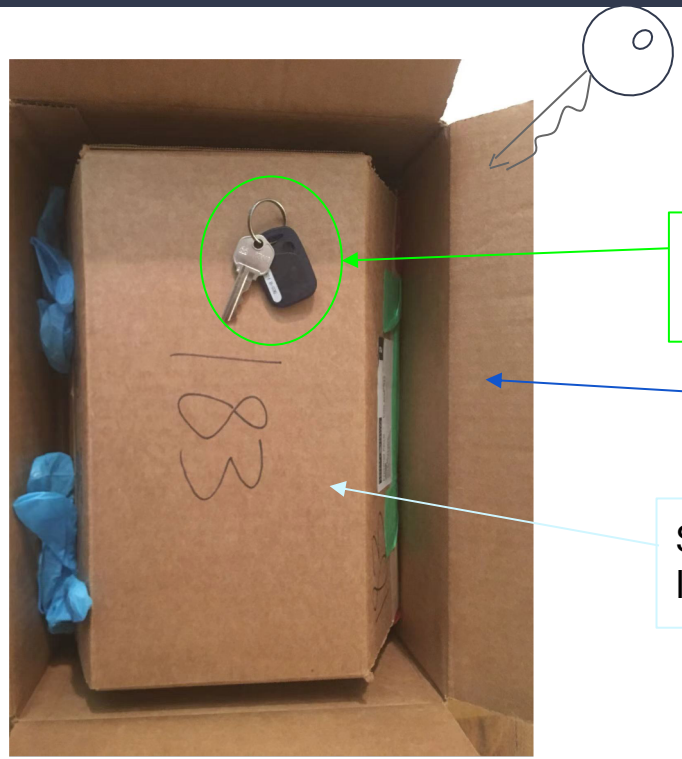
Put the previous box and its key into another box





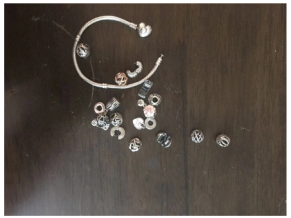
In box 2, there is box 1 and box 1's key. Therefore, the worker can open box 1 inside box 2, but cannot get the jewelry out of box 2. Because Alice has box 2's key.

Last step



Alice opens the last box with the last key and gets her jewelry!

Only she can take the jewelry out because she's smart and always keeps the outer boxes key!



Original data

Computation

result

=

=

=

Original data

Encryption

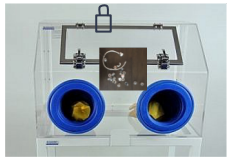
Encrypted data

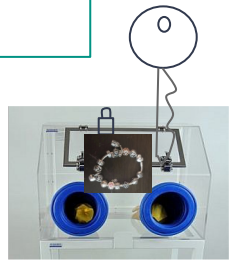
Computation

Encrypted result

Decryption

Decrypted result





So when we look back to homomorphic encryption...

Four Algorithms in Homomorphic Encryption

- *KeyGen*
- *Encrypt*
- *Evaluate*
- *Decrypt*

How do the four algorithms work in HE

- Let’s describe it as symmetric encryption scheme which is easier to understand.
- Also, both plaintext and ciphertext here is binary.
- And say we want to do this with 1100.


BRACE YOURSELVES
MATH IS COMING
AGAIN
memegenerator.net

How do the four algorithms work in HE

^{8} : security parameter (set by the user)

a,b: randomly generated by the algorithm

For the purpose of demonstration, we set ^{8} **!=** 2, ***a*** *>!3-!*and ***b*** *>!6*

N *>!**λ*** *>!3*
P *>!$^{8\ a}$ >!3^{2} >!5*
Q *>!**λ**^{b} >!3^{5} >!43*

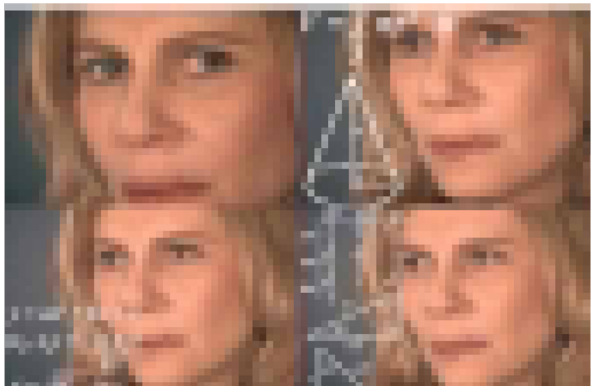
How do the four algorithms work in HE

$p \in [1, \lambda^P - 1] \Rightarrow p \in [1, 2^4 - 1] \Rightarrow p \in [1, 15]$

$p \% 2 == 1 \Rightarrow p$ *is odd*

$q \in [0, \lambda^Q - 1] \Rightarrow q \in [0, 2^{32} - 1] \Rightarrow q \in [0, 4294967295]$

q could be different for each bit of the plaintext



How do the four algorithms work in HE

p	7	7	7	7
plaintext	1	1	0	0
q	13	2526	2022	26
ciphertext	92			

ciphertext = plaintext + ***p * q***

92 = 1 + 7 * 13

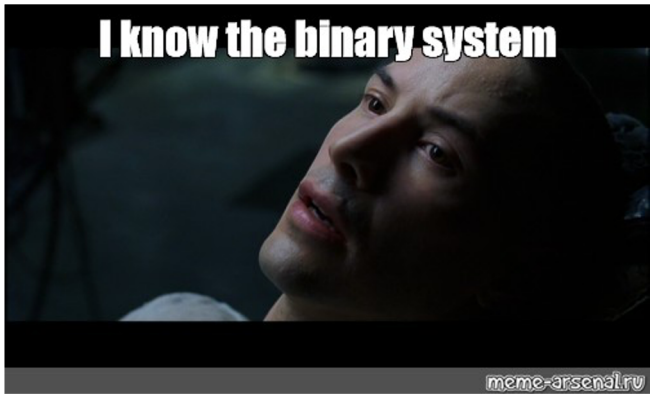
How do the four algorithms work in HE

Now let’s convert 92 back to binary!

ciphertext[0] = 1011100

It needs to be ***N + Q*** = 2 + 32 = 34 bits long (i.e. padding)

Therefore ciphertext[0] = 0000000000000000000000000001011100



How do the four algorithms work in HE

- *Evaluate*
  - Computations
  - For FHE, it should include everything
  - For partially and somewhat, they cannot.

How do the four algorithms work in HE

ciphertext[0] = 00000000000000000000000001011100 = 92

Now let’s decrypt it!

plaintext[0] = (ciphertext[0] mod ***p***) mod 2 = (92 mod 7) mod 2 = 1 mod 2 = 1

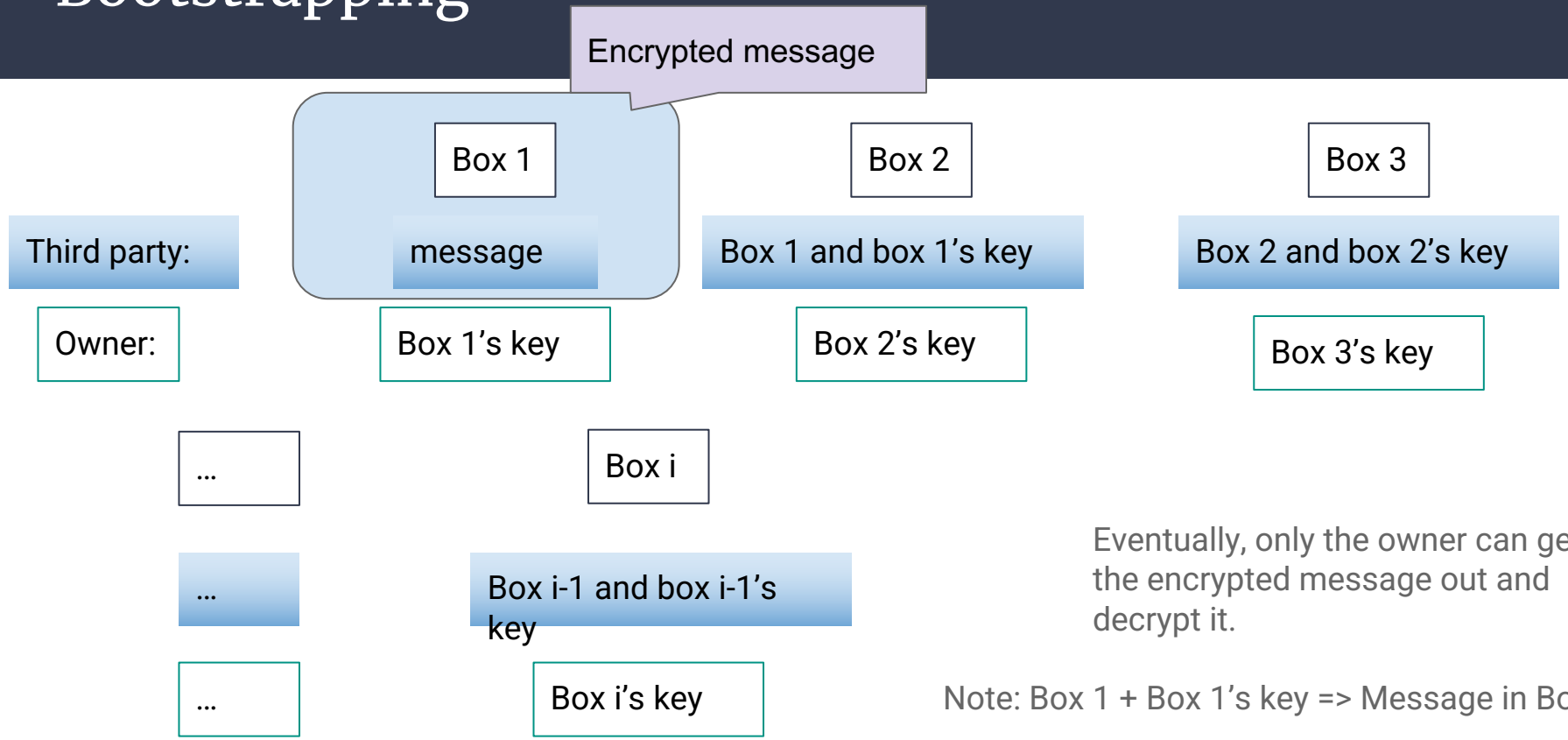
However, the operations(*evaluate* part) increase the noise associated to resulting ciphertexts.

Therefore, after several operations, the noise could become large enough that decryption is no longer reliable.

Bootstrapping

- reduce the error without decrypt in the middle
- Only for fully homomorphic encryption

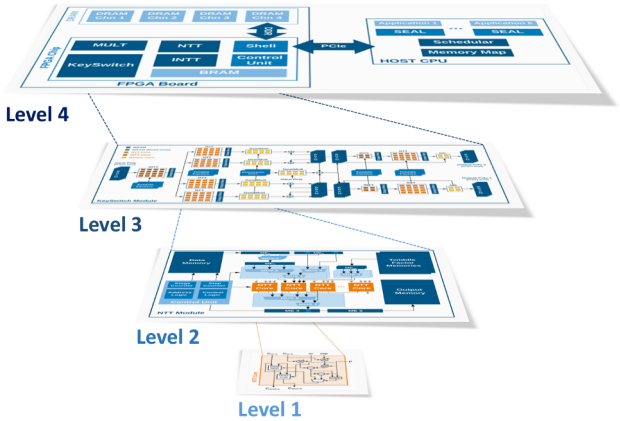
Bootstrapping



Eventually, only the owner can get the encrypted message out and decrypt it.

Note: Box 1 + Box 1's key => Message in Box 2

Future directions



Microsoft's project Heax

Designing a new computing architecture, specifically designed for FHE.

Cloud computing and storage!

References

1. https://blog.openmined.org/from-fully-homomorphic-encryption-to-silicon/
2. https://en.wikipedia.org/wiki/Encryption
3. https://www.techtarget.com/searchsecurity/definition/encryption
4. https://medium.com/searchencrypt/what-is-encryption-how-does-it-work-e8f20e340537
5. http://blog.higashi.tech/2020/06/22/fhe_02.html
6. https://www.cleatech.com/product-category/glove-box-system/portable-glove-boxes/
7. https://crypto.stanford.edu/craig/craig-thesis.pdf
8. https://crypto.stanford.edu/craig/easy-fhe.pdf
9. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
10. https://cryptobook.nakov.com/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc
11. http://blog.higashi.tech/2020/06/16/fhe_01.html
12. https://en.wikipedia.org/wiki/Homomorphic_encryption
13. https://www.geeksforgeeks.org/implementation-diffie-hellman-algorithm/

References

- Shout out to whoever made those memes, you have my 100% respect

Thank You!