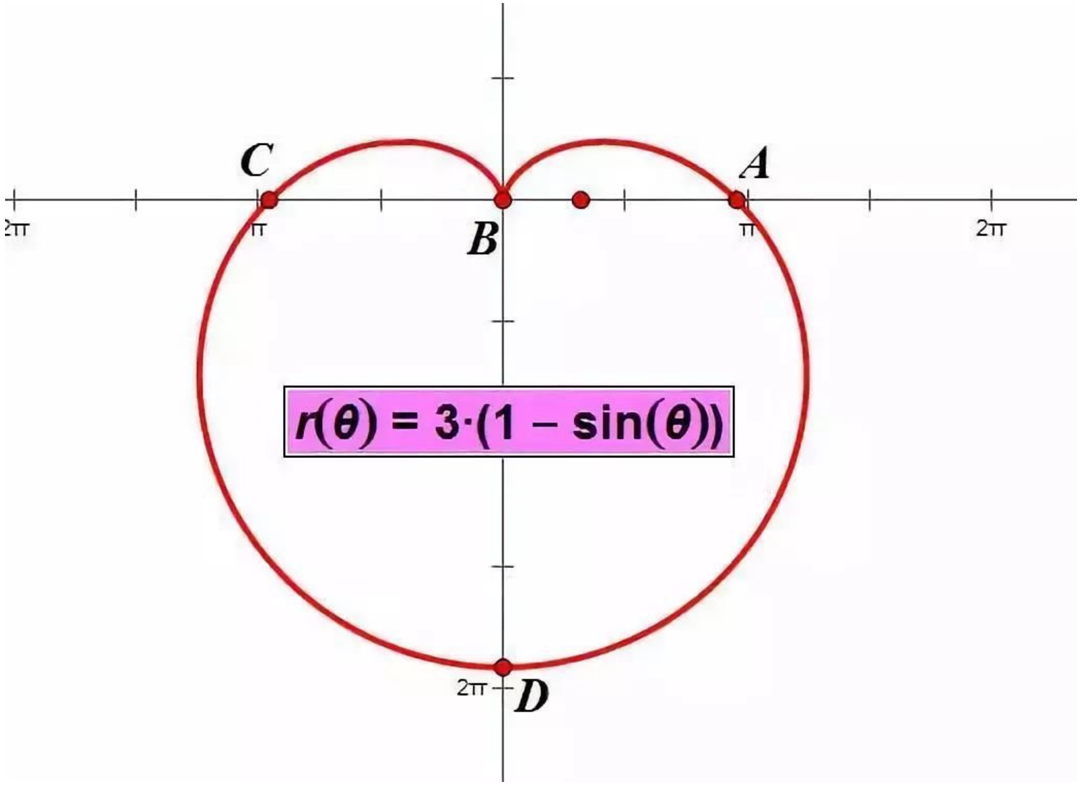
Technologies for E-Commerce

CAN302

Department of Communications and Networking

Xi’an Jiaotong-Liverpool University (XJTLU)

Week9 – Encoding and Encryption



$Mg + ZnSO4 = Zn + MgSO4$

Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key.

https://www.sohu.com/a/294741873_702480

Outline

1. Ancient encryption
2. Symmetric and Asymmetric encryptions

Ancient encryption

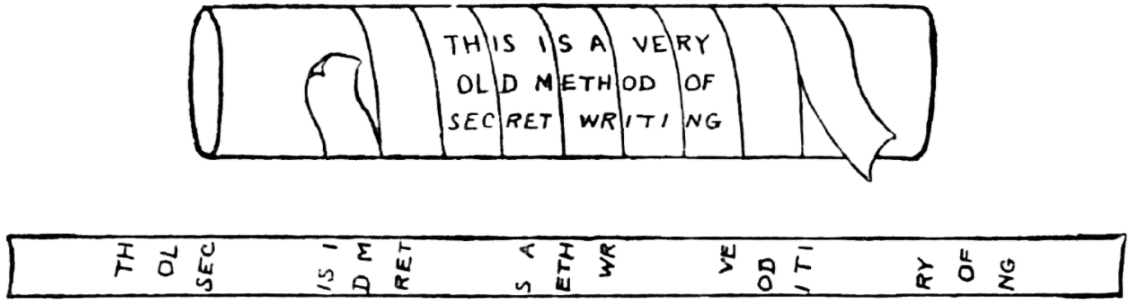
芦花丛中一扁舟，

俊杰俄从此地游。

义士若能知此理，

反躬难逃可无忧。

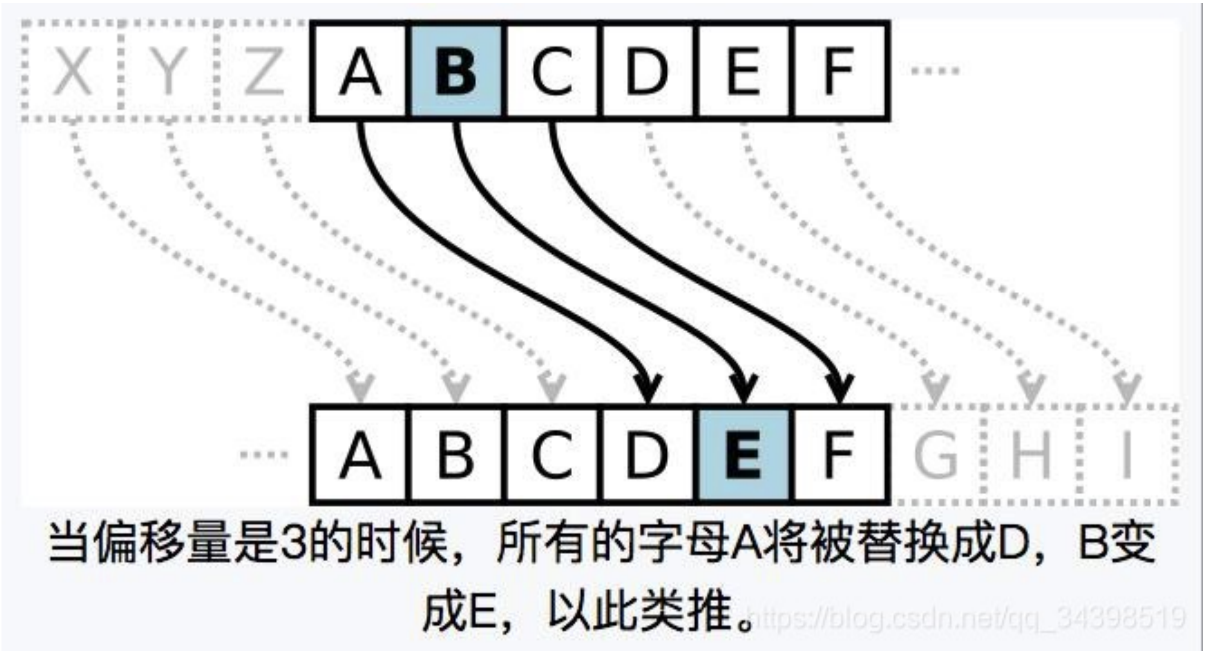
--水浒传



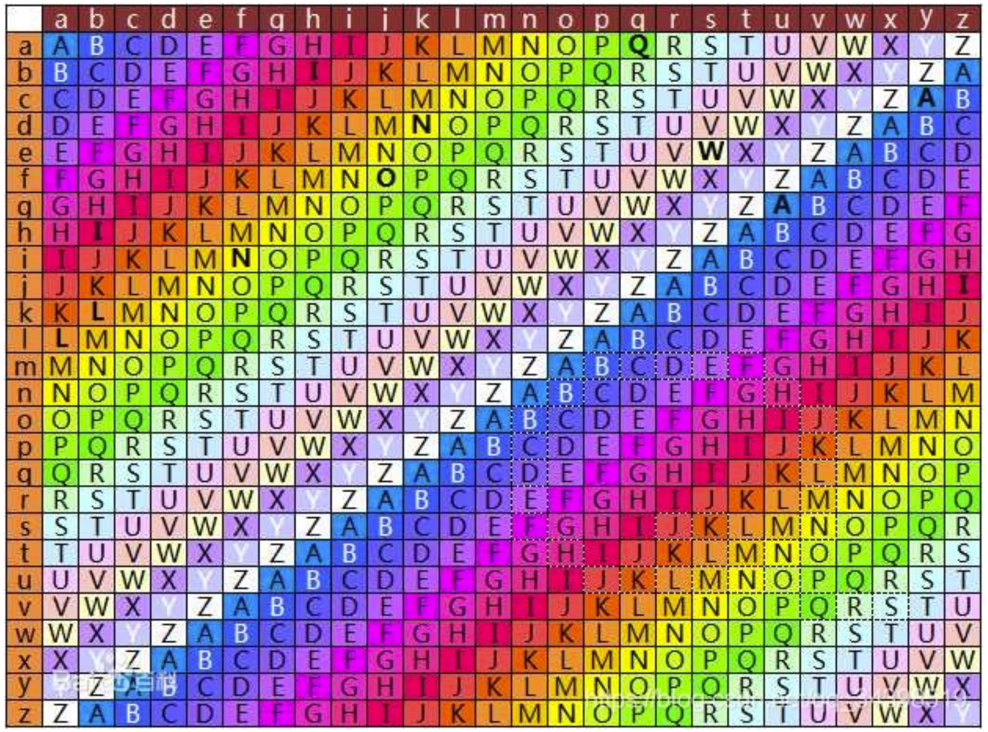
The **Scytale** Cipher was used in ancient Greece by the Spartans in which a band was wrapped around a rod, and a message was written.

https://www.forthright.com/a-guide-to-encryption-history-how-it-works-and-why-you-need-it/

Ancient encryptions



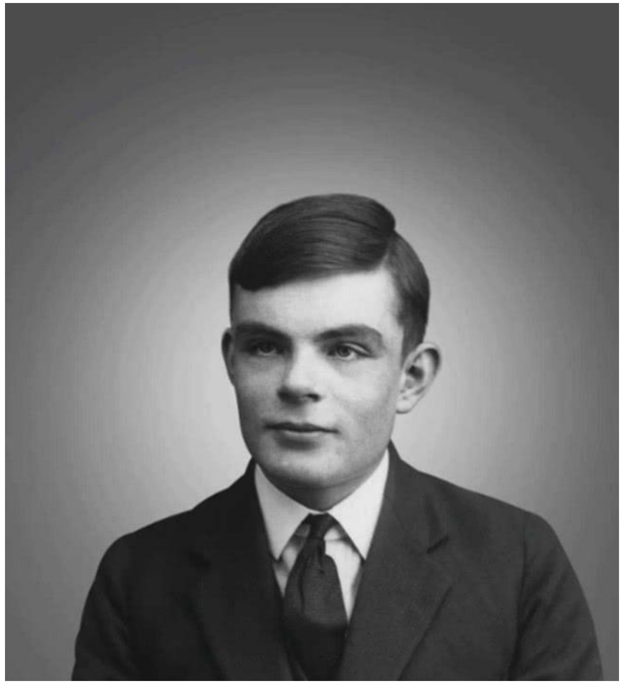
Caesar cipher

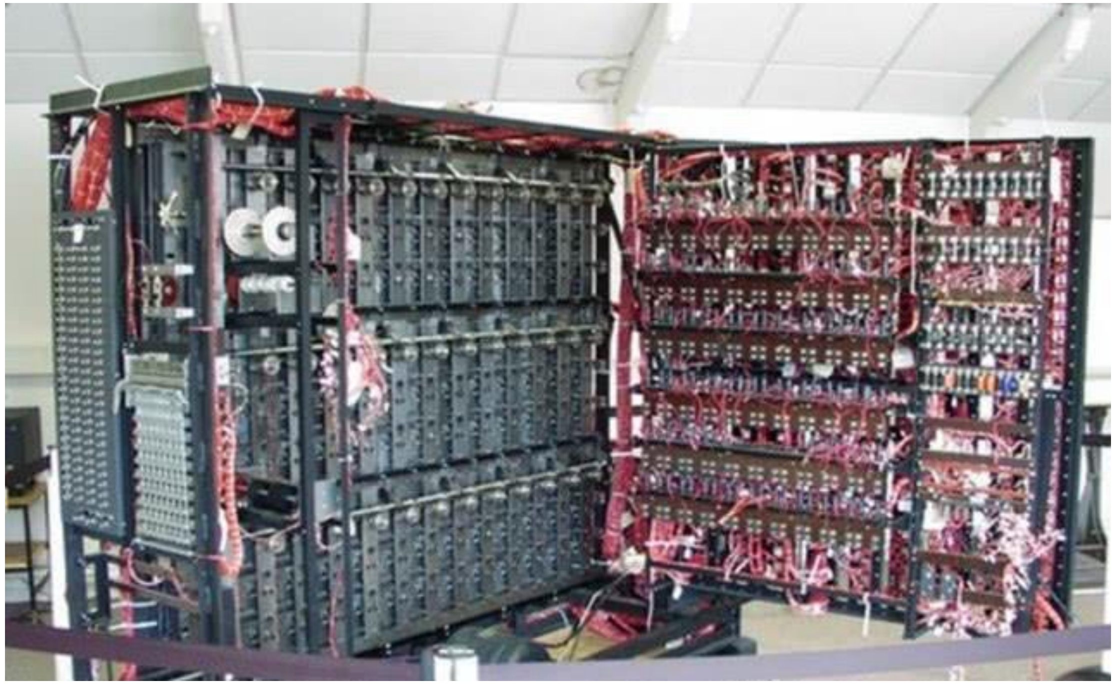


The Vigenere cipher

https://blog.csdn.net/qq_34398519/article/details/115412600
https://www.bilibili.com/video/av71024212/

Security is always: "The code"



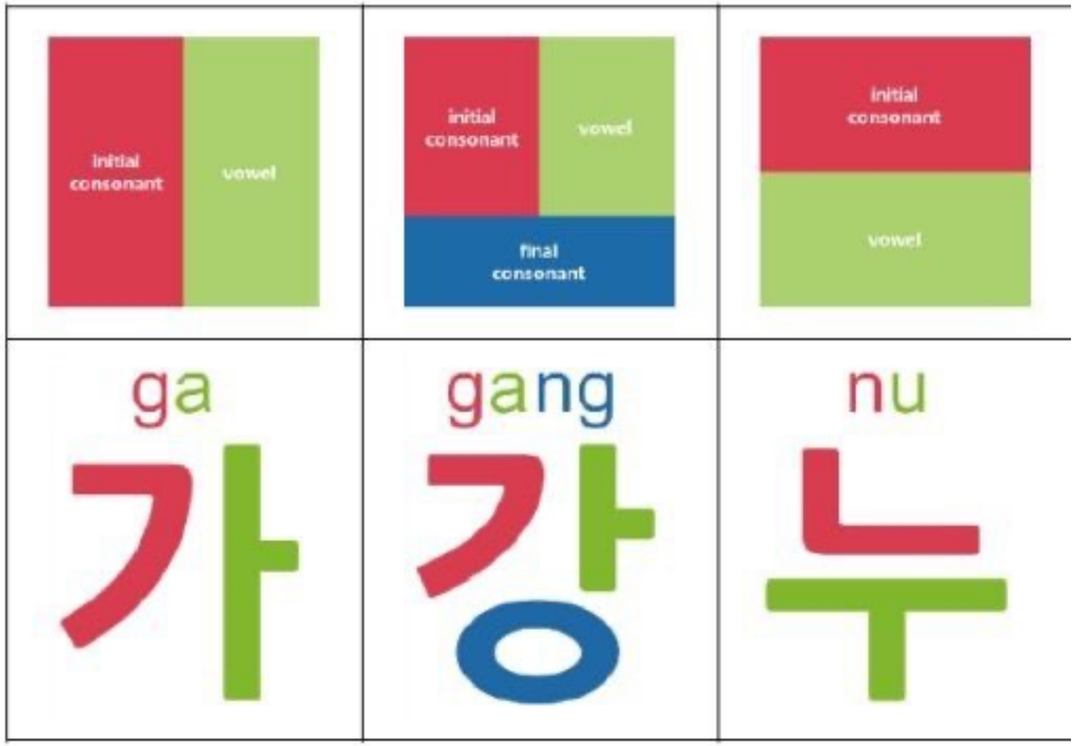


Alan Mathison Turing, 1912 - 1954

Enigma machine

https://www.sohu.com/a/443659675_120339167
https://www.163.com/dy/article/EHTEK00805372PI2.html
https://www.163.com/dy/article/GDC5UVCC0543U41J.html
https://item.jd.com/12307986.html

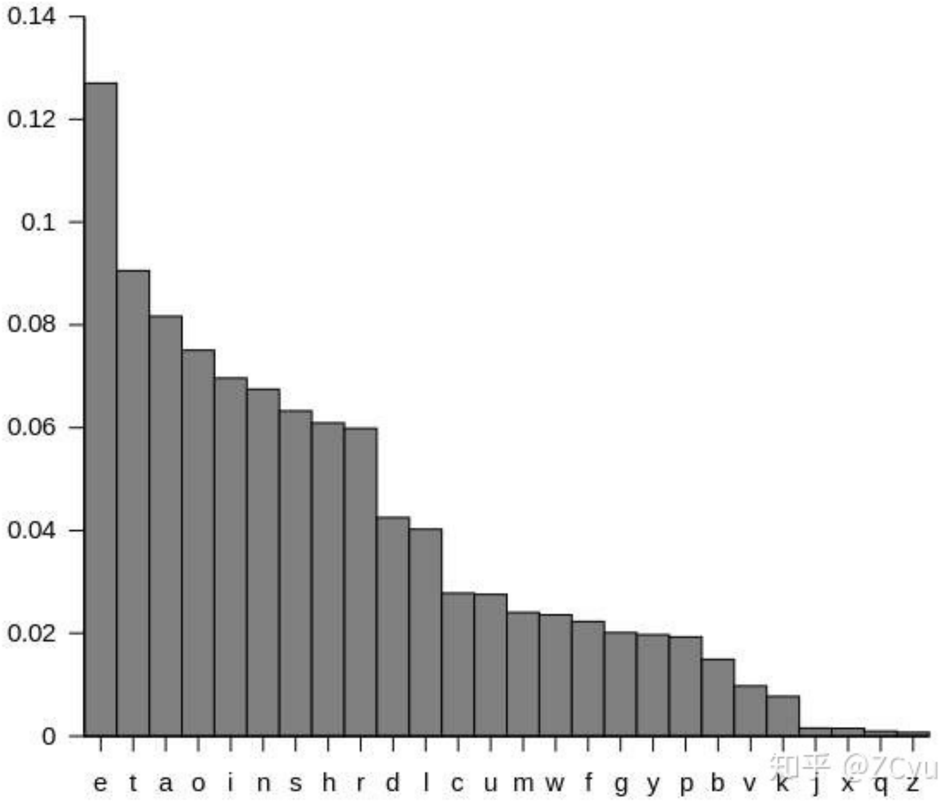
Types of language



	linguistic structure	orthographic structure
meaning-based	text	—
	topic	—
	speech act	pictorial signs
	word	logographic writing
	morpheme	
sound-based	syllable	syllabic writing
	segment	consonantal writing
	phoneme	alphabetic writing
	phone	phonetic alphabet
	feature	featural writing system

https://www.britannica.com/topic/writing/Types-of-writing-systems
https://www.zhihu.com/question/21777680/answer/136676230
https://aminoapps.com/c/korean--school/page/blog/quick-guide-to-hangeul-hangeul/d35k_XowSbu1Y68GJxMnoDRJNIboZvK0m4g

Crack the encryption



字母	英语中出现的频率
e	12.702%
t	9.056%
a	8.167%
o	7.507%
i	6.966%
n	6.749%
s	6.327%
h	6.094%
r	5.987%
d	4.253%
l	4.025%

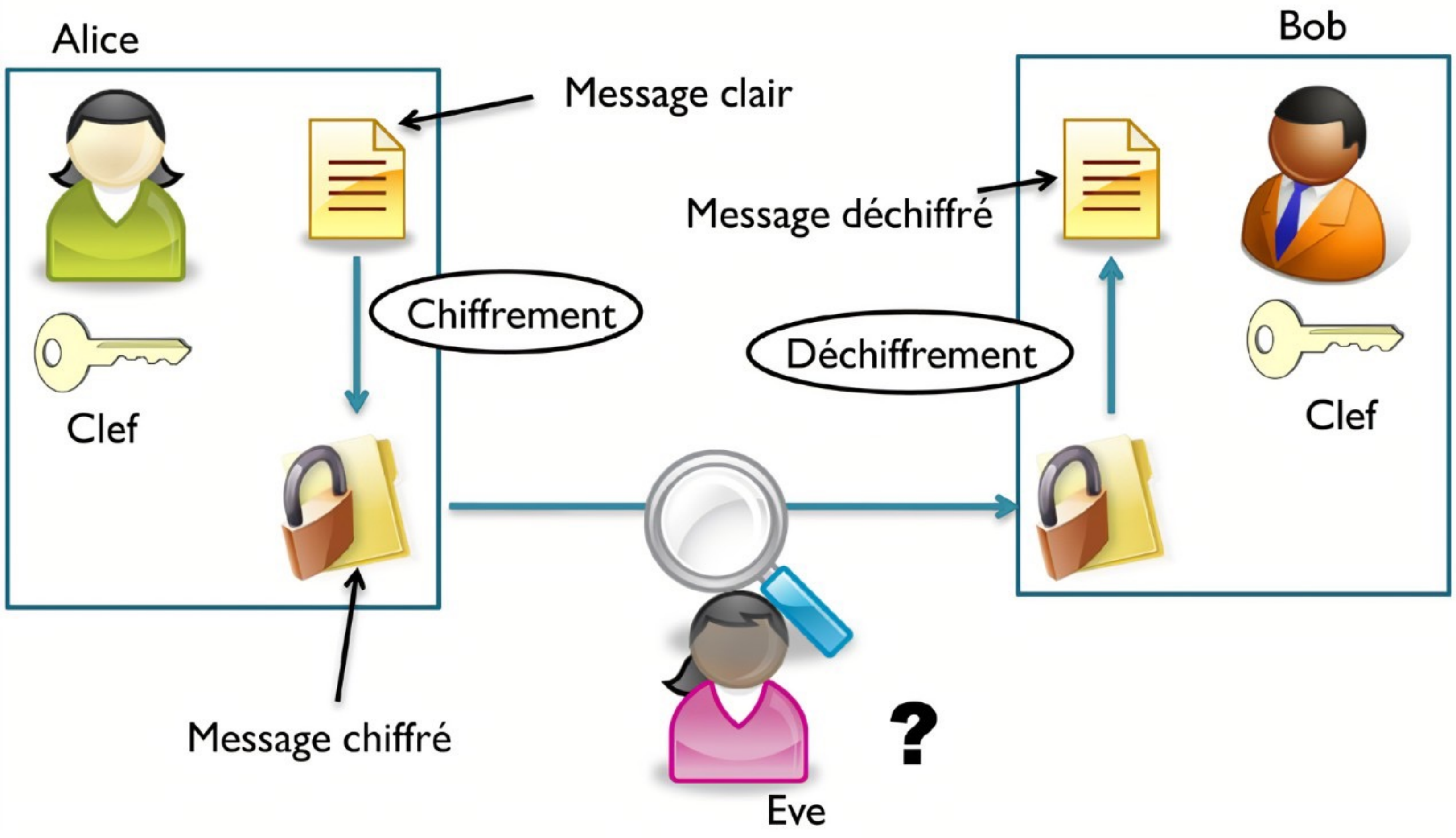
https://zhuanlan.zhihu.com/p/111611977

Dialect is an excellent encryption!

“Wind Talkers”

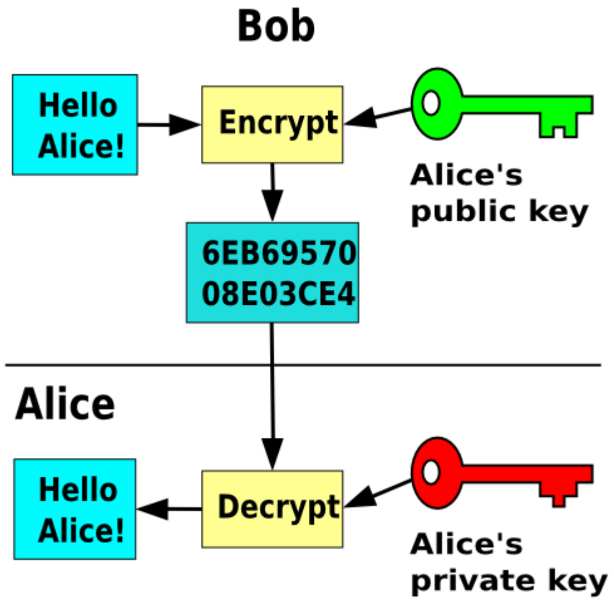
https://www.zhihu.com/question/356444538
https://baijiahao.baidu.com/s?id=1583124320725288717&wfr=spider&for=pc

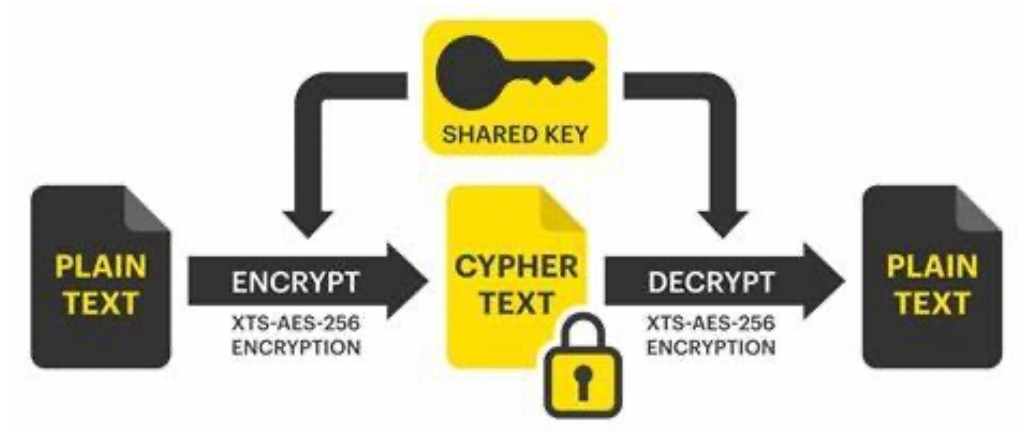
Modern encryption: Bob, Alice and Eve



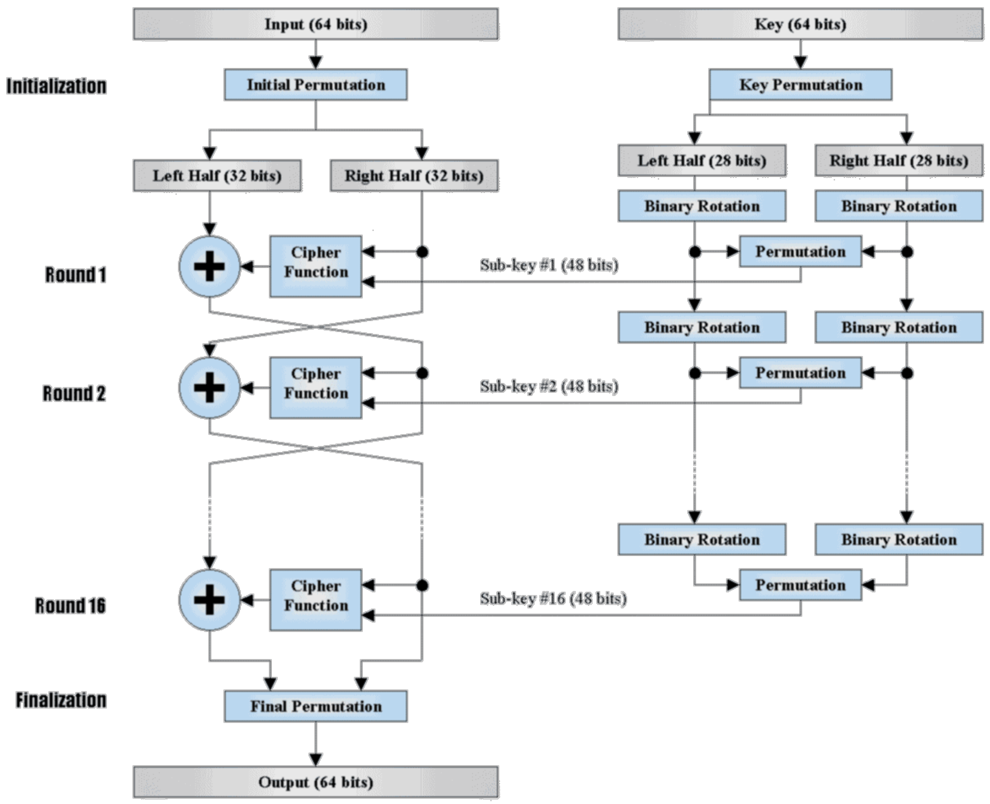
Let's explain it now.

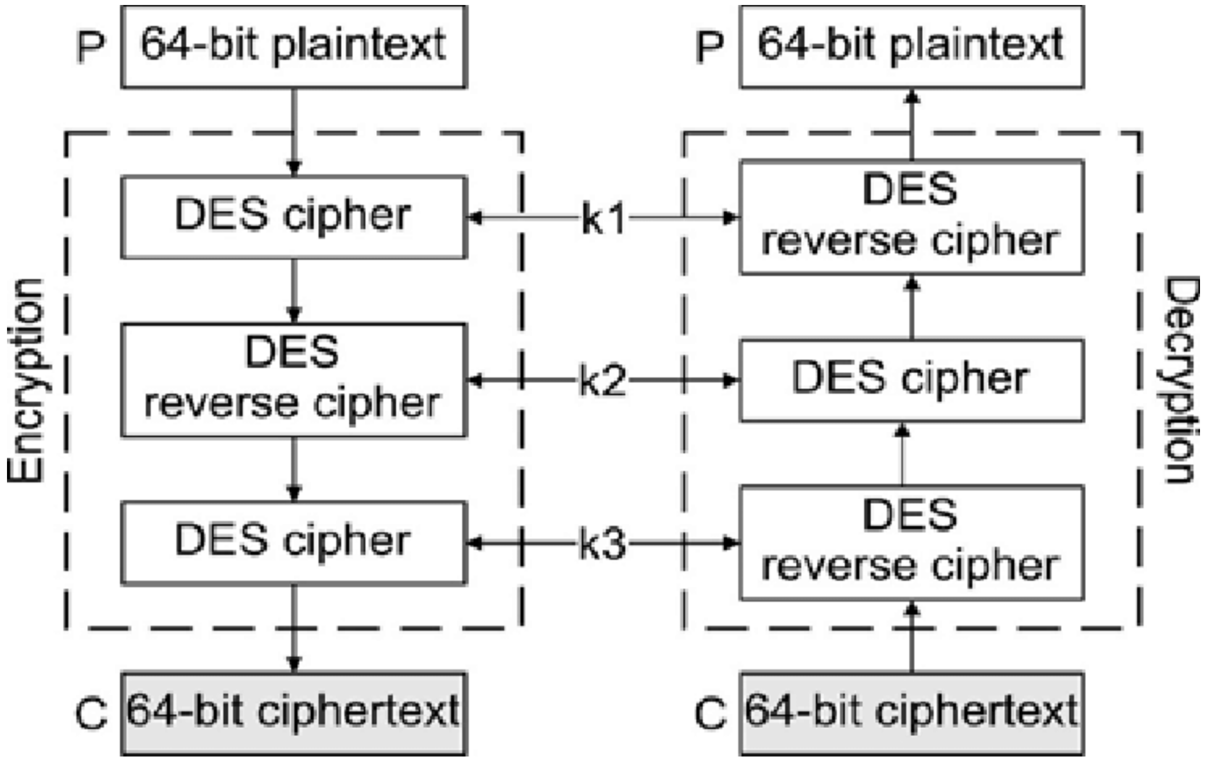
Symmetric and Asymmetric keys





DES (Data Encryption Standard) and 3DES

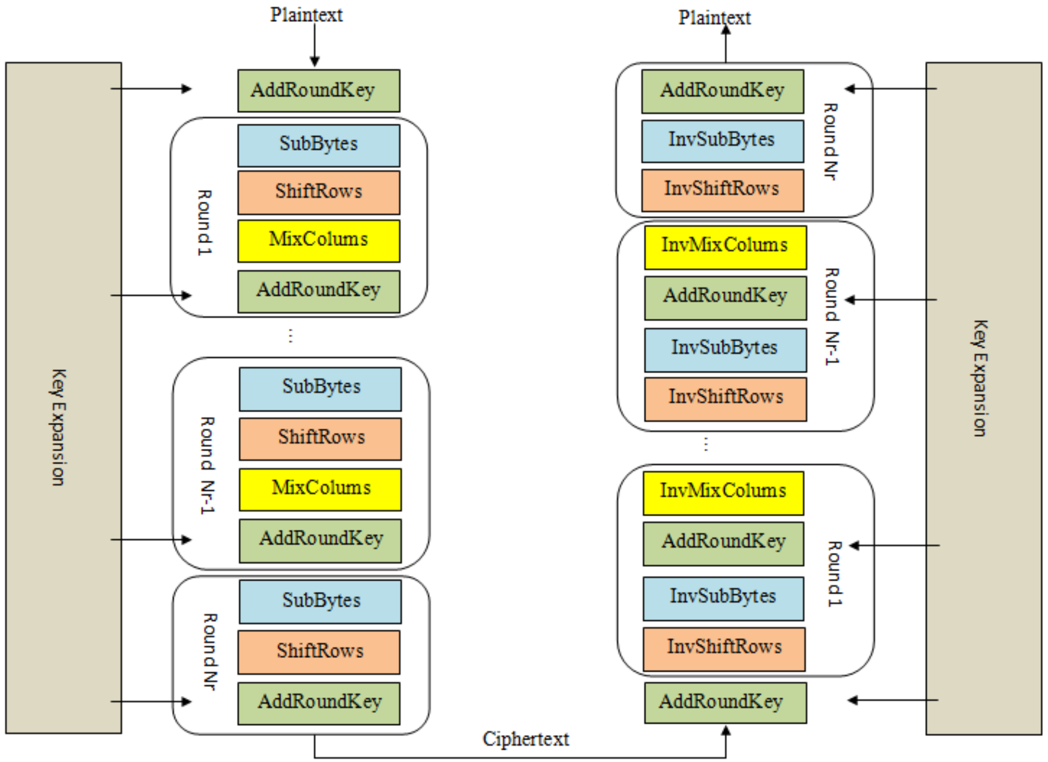


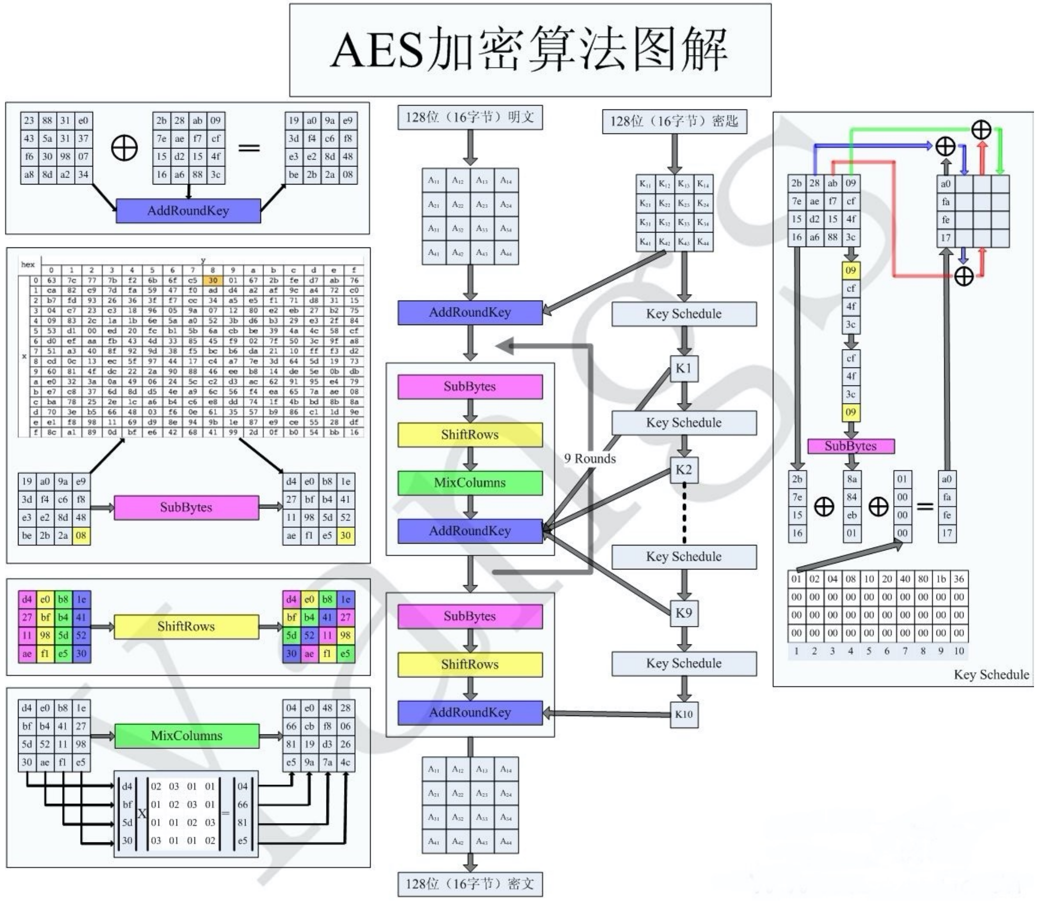


In the early 1970's, IBM realized that their customers were demanding some form of encryption, so they formed a "crypto group" headed by Horst-Feistel. They designed a cipher called Lucifer. In 1973, the Nation Bureau of Standards (now called NIST) in the US put out a request for proposals for a block cipher which would become a national standard.
In 1997, DES is not regarded as safe one due to the length of key. So do it triple times and got 3DES.

https://www.bilibili.com/video/BV1KQ4y127AT
https://www.cnblogs.com/songwenlong/p/5944139.html

AES (Advanced Encryption Standard)





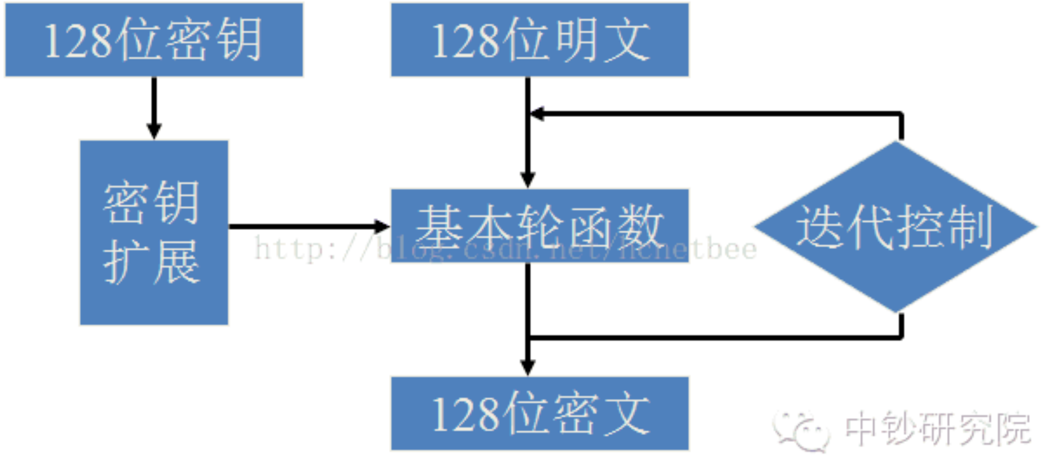
Rijndael is a family of block ciphers developed by Belgian cryptographers Vincent Rijmen and Joen Daemen. It was submitted as an entry to the National Institute of Standards and Technology's (NIST) competition to select an Advanced Encryption Standard (AES) to replace Data Encryption Standard (DES).

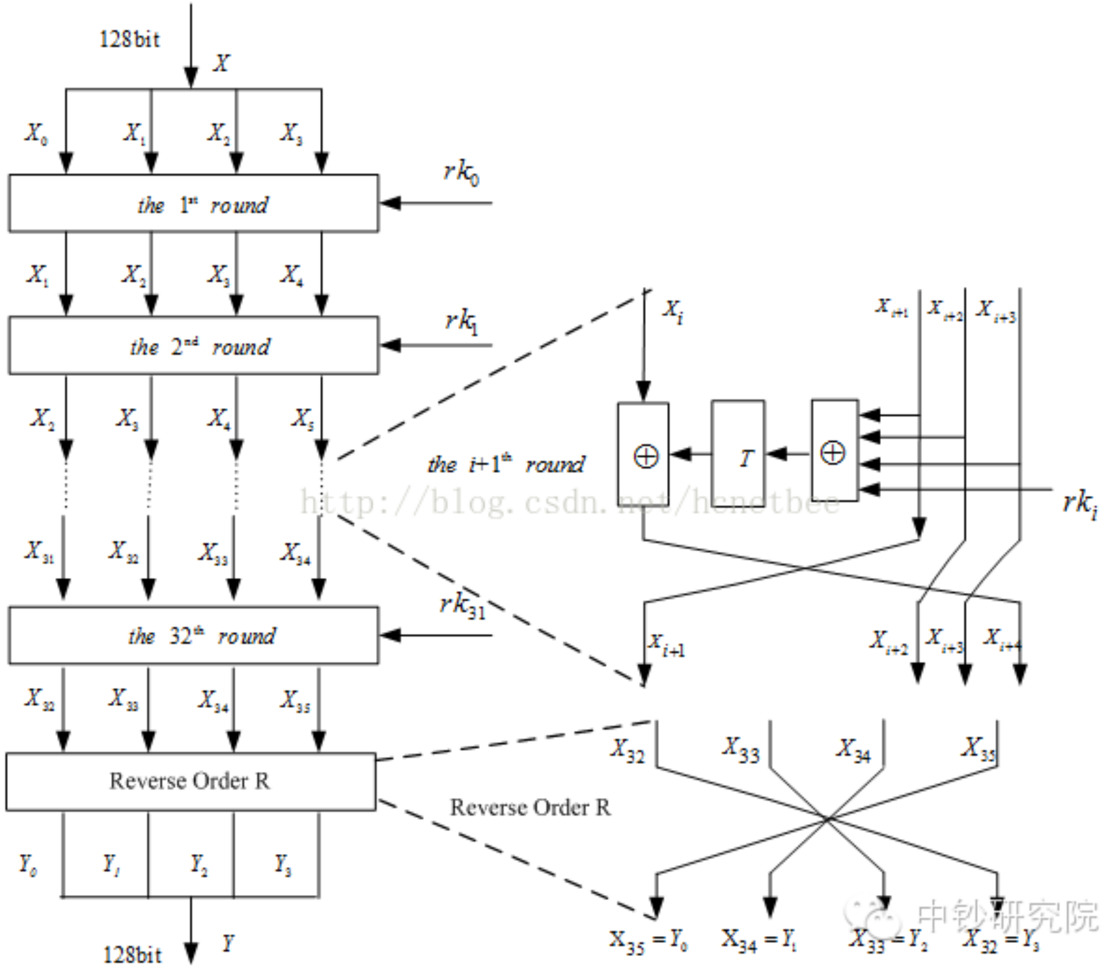
https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5
https://www.bilibili.com/video/BV1i341187fK/?spm_id_from=333.788.b_7265636f5f6c697374.2

Chinese algorithms of symmetric encryption

国家密码管理局

WWW.SCA.GOV.CN

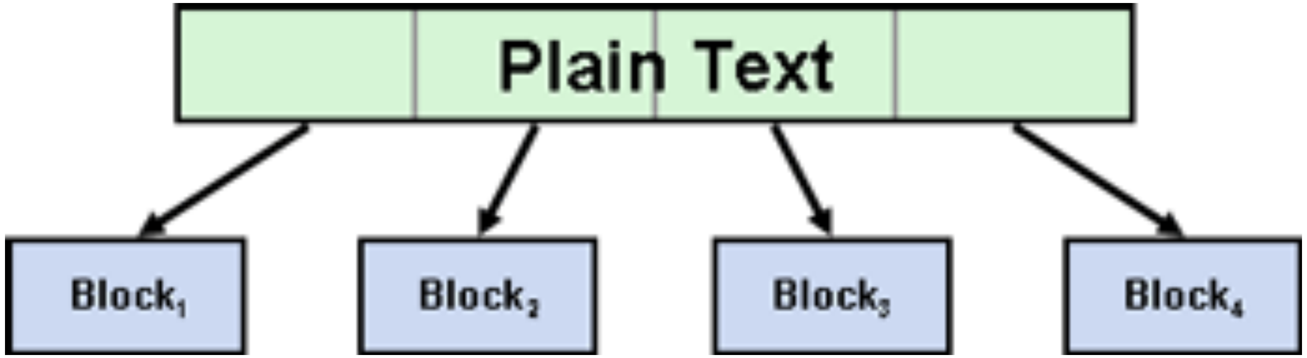




- SM1 is not open to public.
- SM4 is similar to AES.
- SM7 and ZUC are two new algorithms.

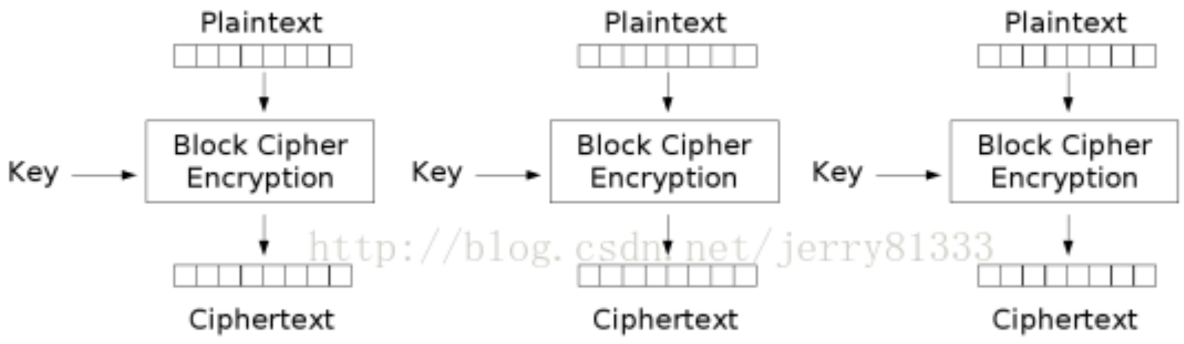
https://blog.csdn.net/andylau00j/article/details/80102983
https://www.sohu.com/a/288876376_100078137

Block cipher

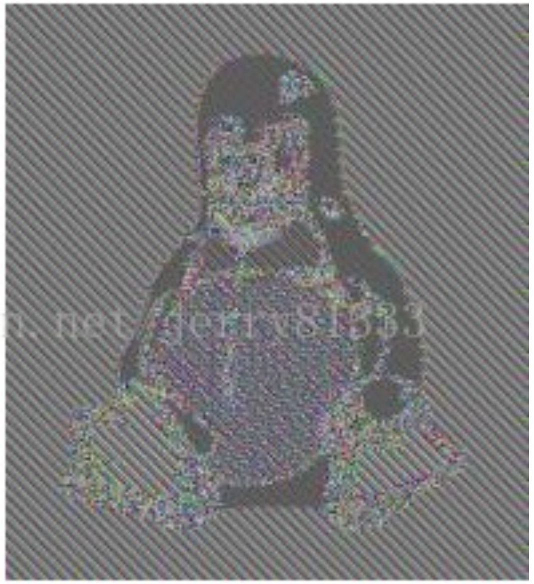


- The data need to be put in blocks

Block cipher modes



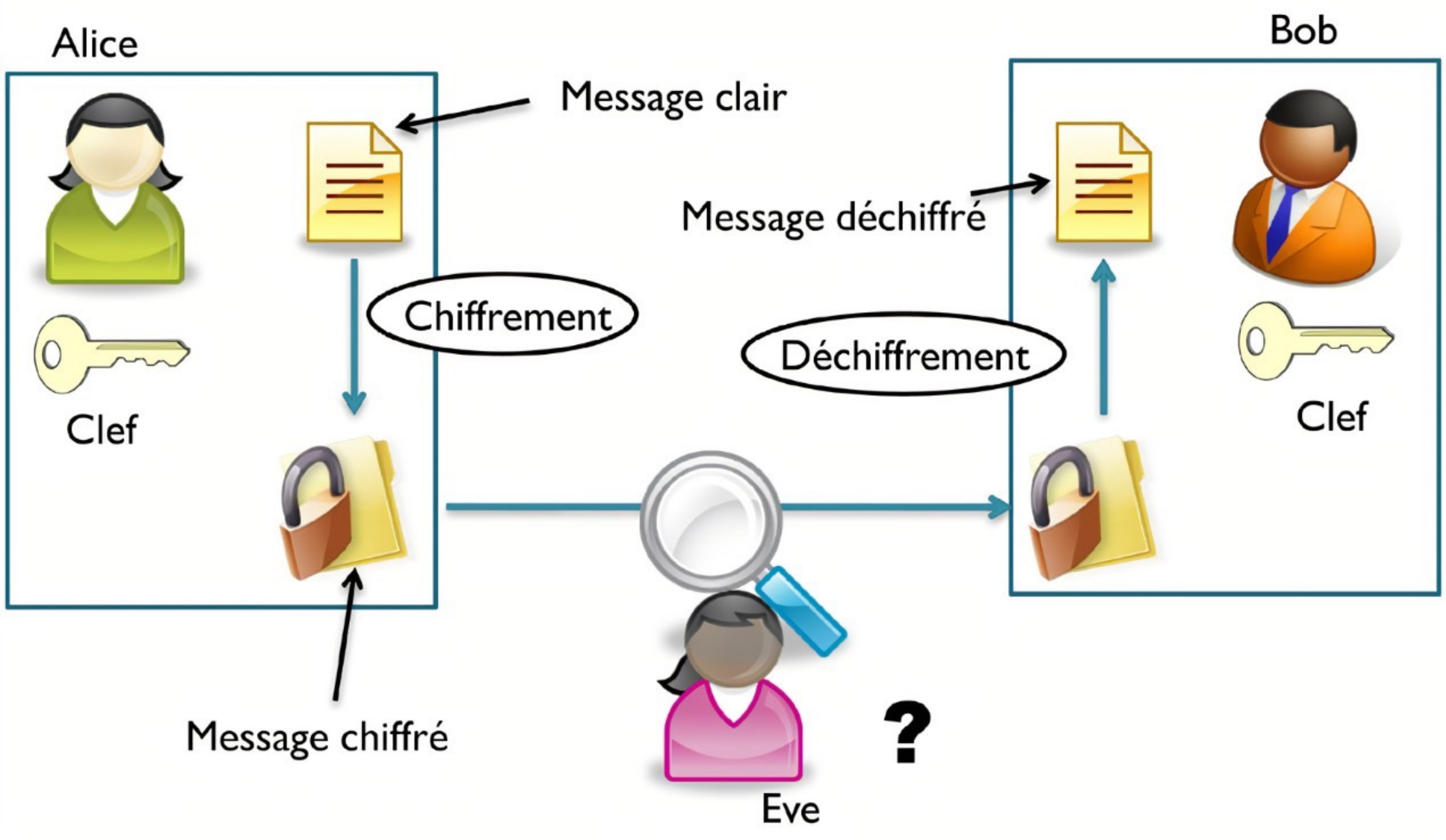
Electronic Codebook (ECB) mode encryption



- ECB is most simple one but sometime it is not good enough.
- There are many other modes like **CBC、PCBC、CFB、OFB、CTR**
- No good or bad between different modes, it depends on applications.

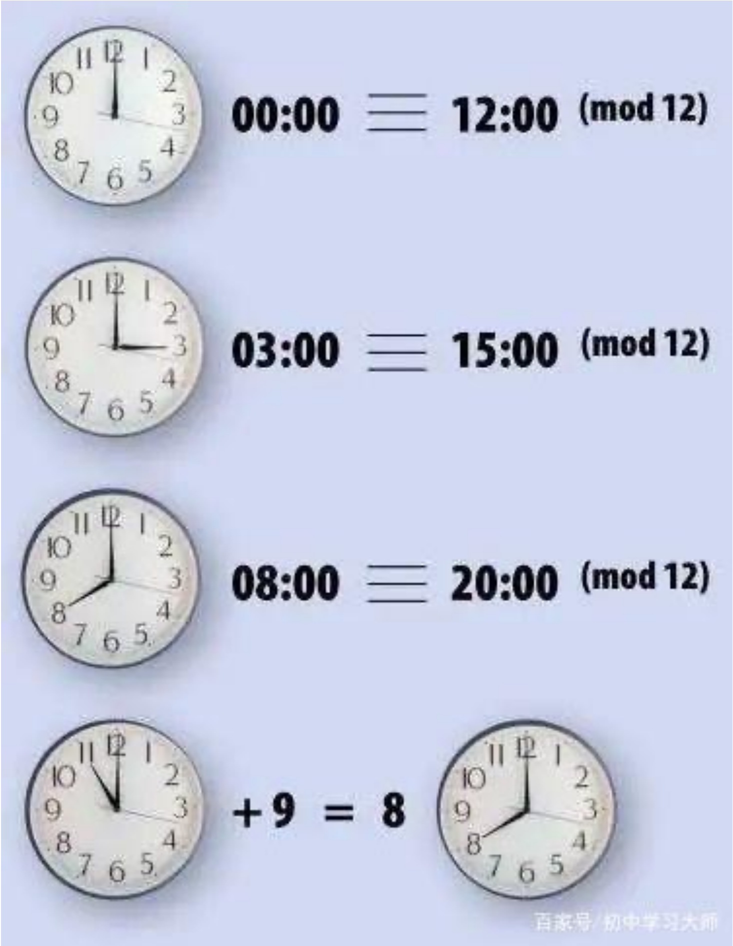
https://blog.csdn.net/jerry81333/article/details/78336616

Next challenge: exchange the keys safely



Let's explain it now.

^ and % - a basic math for encryption



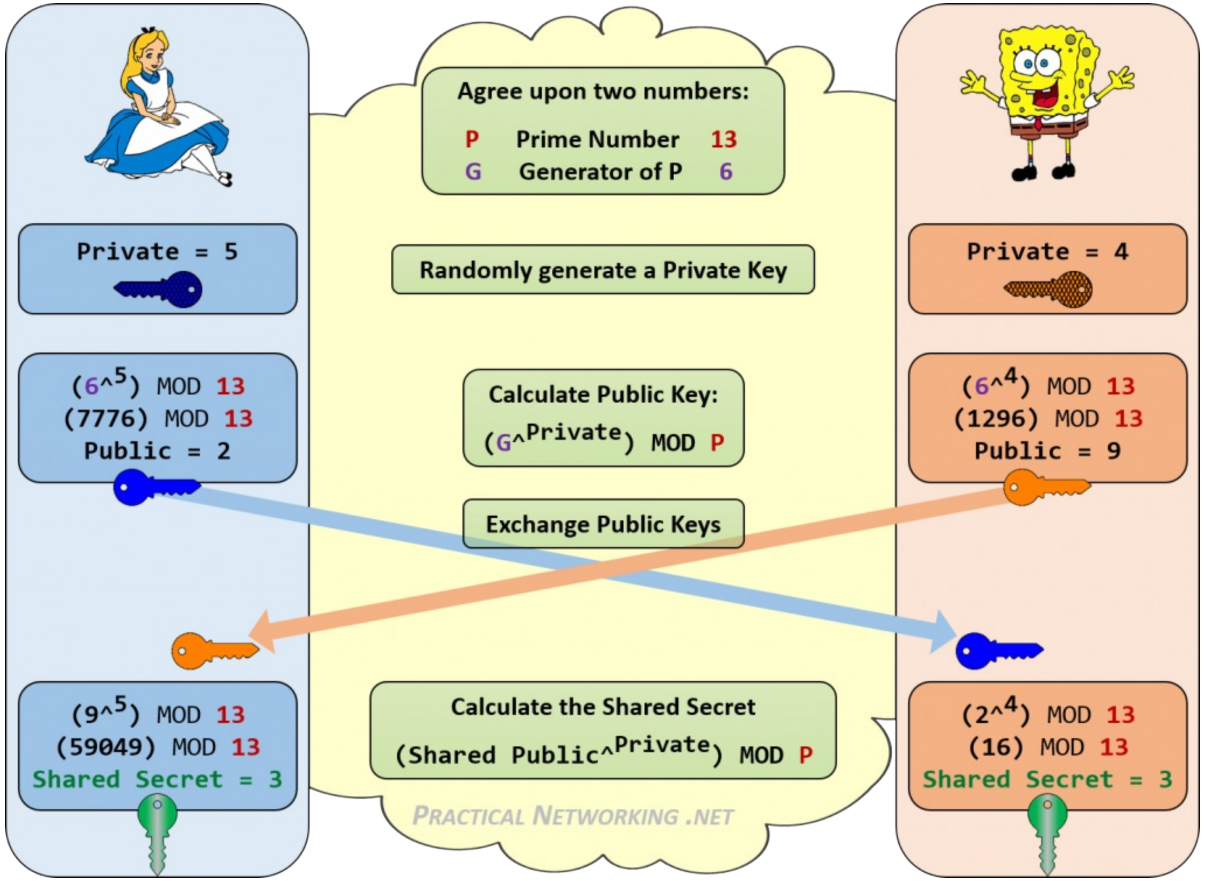
$$(a^b)\%p = (q^b)\%p$$

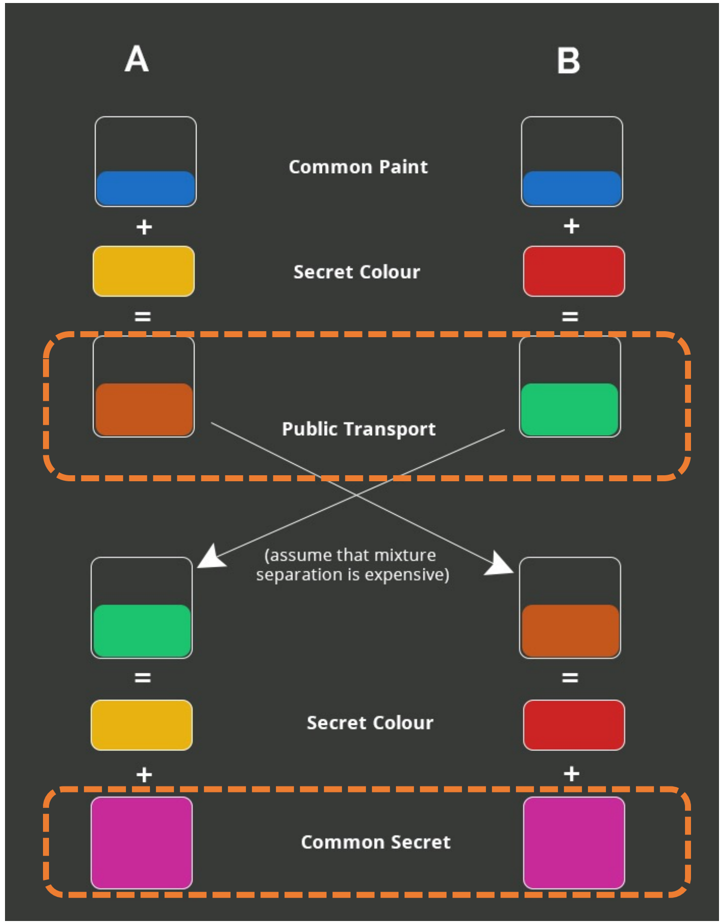
$$a = mp + q$$

$$a^b = (mp+q)^b = C_b^0(mp)^b + C_b^1(mp)^{b-1}q + \cdots + C_b^b q^b$$

https://baijiahao.baidu.com/s?id=1712774547215656066&wfr=spider&for=pc

Diffie–Hellman algorithm

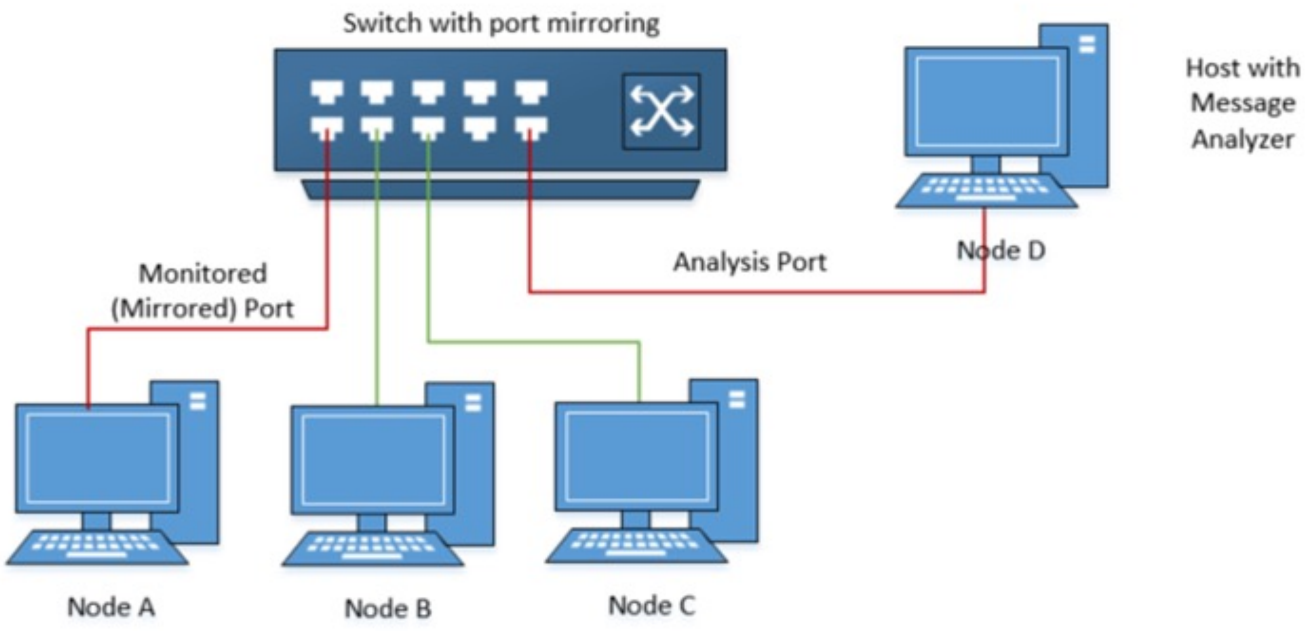


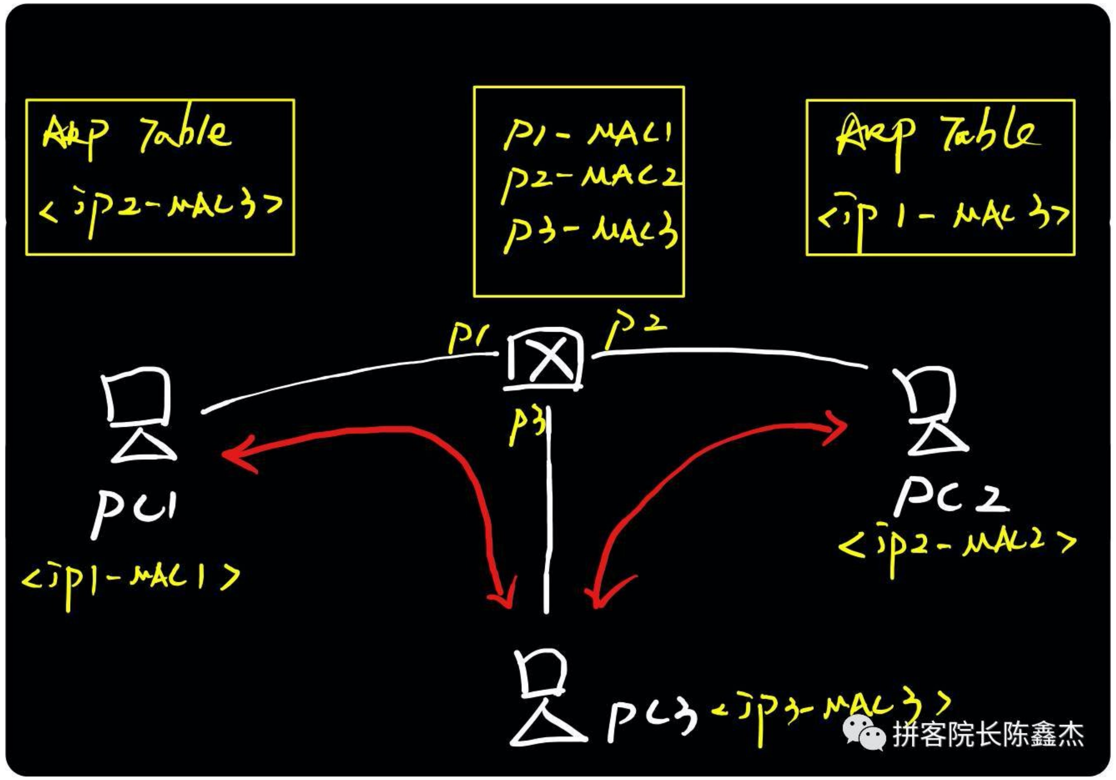


- **Basic idea is about certain math difficulties.**
- **Exchange (g^a mod p) mod and (g^b mod p)**
- **Key = g^{ab} mod p = (g^a mod p)^b mod p = (g^b mod p)^a mod p**

http://www.practicalnetworking.net/series/cryptography/diffie-hellman/

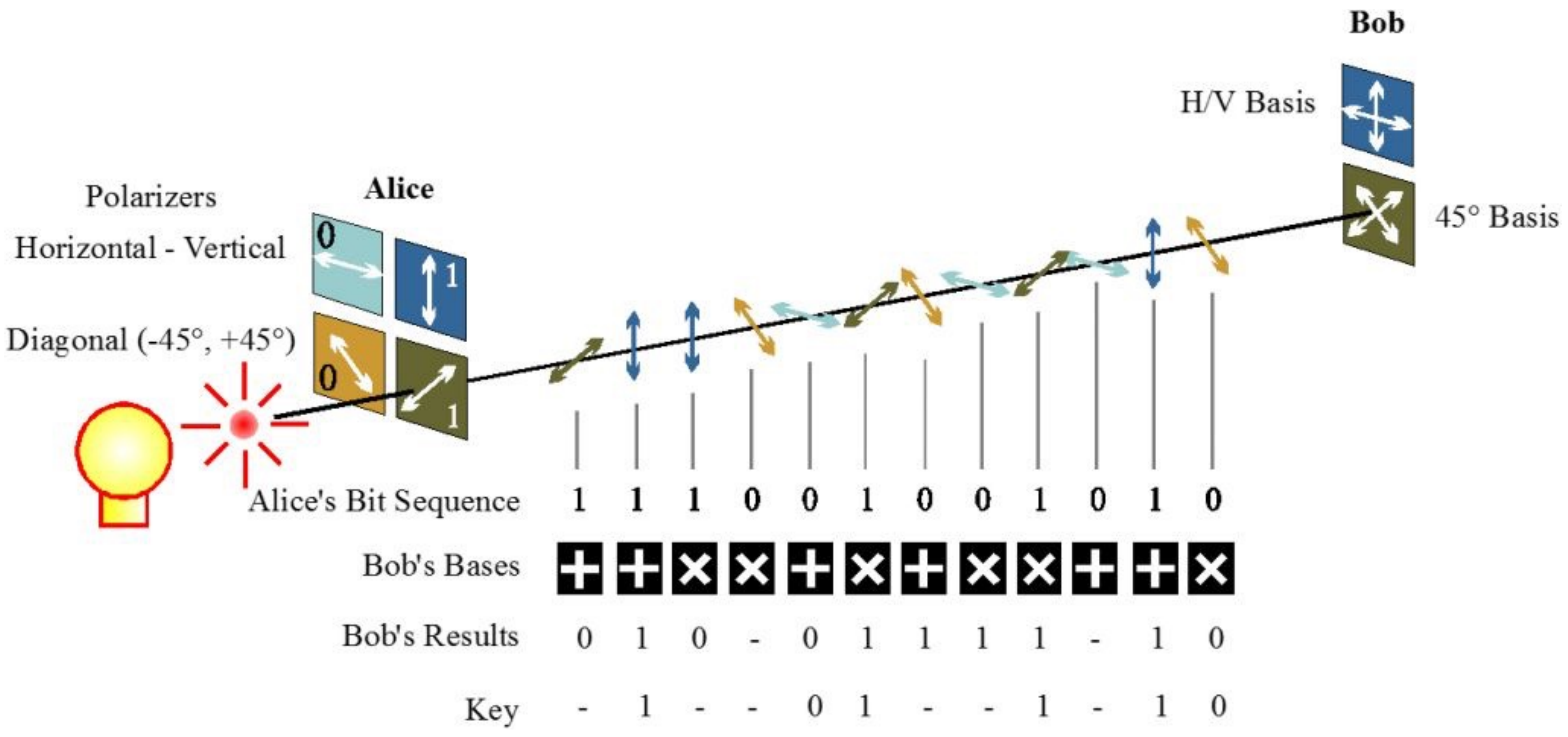
Still cannot against Middle-men!





https://zhuanlan.zhihu.com/p/28818627
https://dun.163.com/news/p/233ea1ba40a14791a5fb8d3b6847b663

Quantum key CAN against Middle-men!



https://www.qtumist.com/post/2178

Asymmetric keys algorithms

- Basic math challange is similar to DH.
- There are very easy “add, minus and plus” but damned hard “divide”.

RSA mechanism

Rivest, Shamir and Adleman @1977

- g is the secret info
- g^a mod p = A, in which (a, p) is one key
- A could be the encrypted info
- If g^{ad} mod p = g,
- A^d mod p = g, in which (d, p) is another key

- Nee to find the proper a, d and p meet g^{ad} mod p = g

- **Still about the ^ and %**
- **But in a different way to apply the math**

Euler's totient function & Fermat's little theorem

- g is the secret info
- g^a mod p = A, in which (a, p) is one key
- If g^{ad} mod p = g,
- A^d mod p = g, in which (d, p) is another key
- Nee to find the proper a, d and p meet g^{ad} mod p = g

Euler's Totient function φ(x) for an input x is the count of numbers in {1, 2, 3, ⋯, n} that are relatively prime to x.

When x is prime, then φ(x) = x -1
When m and n and prime, then φ(m*n) = (m - 1) * (n - 1)

Euler theorem g^φ(p) mod p = 1 (g could be any number)

Since $g^{k\varphi(P)}$ mod p = 1 and $g^{k\varphi(P)+1}$ mod p = g, then d = (kφ(p)+1)/a

Let p = m*n, it is easy to have a set of a (choosing), d (deduced) and p (caculating) for our key pairs.

https://www.jianshu.com/p/878ac7ea196b

A demo of RSA keys

- $g^{k\varphi(p)+1} \bmod p = g$ and $d = (k\varphi(p)+1)/a$
- Let p = m*n, to get a set of a, d and p for key pairs as: {a, p} and {d, p }

(1) select m = 29, n = 83

(2) p = 29 * 83= 2407, φ(p) = (29 -1) * (83 - 1) = 2296

(3) Select a = 5

(4) Choose k = 4, d = (4 * 2296 + 1) / 5 = 1837

(5) Key pair is｛5, 2407｝and｛1837, 2407｝

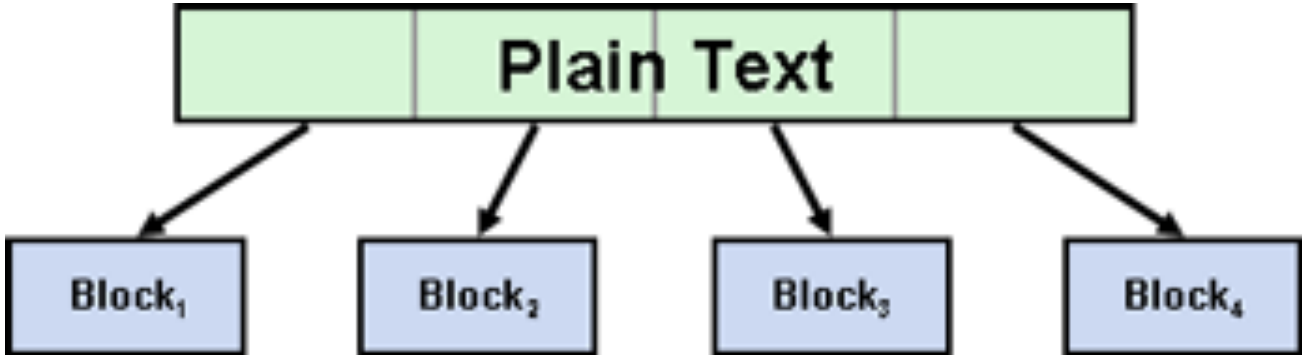
Testing:

Plain number: num = 2

Encryption it NUM = 2^1837 (mod 2407) = 2312

Decryption num' = 2312^5 (mod 2407) = 2

Block cipher again



- If the data length beyond the key length, it also needs to be put in blocks

Challenge to crack RSA keys

- For key pairs {a, p} and {d, p }, we would publish the {a, p} and keep {d, p } as secret.
- We get d from $d = (k\varphi(p)+1)/a$ easily.
- Eve need to know $\varphi(p)$ to get d.
- So Eve need to find out the m and n which fits $p = m * n$.

12301866845301177551304949
58384962720772853569595334
79219732245215172640050726
36575187452021997864693899
56474942774063845925192557
32630345373154826850791702
61221429134616704292143116
02221240479274737794080665
351419597459856902143413

33478071698956898786044169
84821269081770479498371376
85689124313889828837938780
02287614711652531743087737
814467999489

×

36746043666799590428244633
79962795263227915816434308
76426760322838157396665112
79233373417143396810270092
798736308917

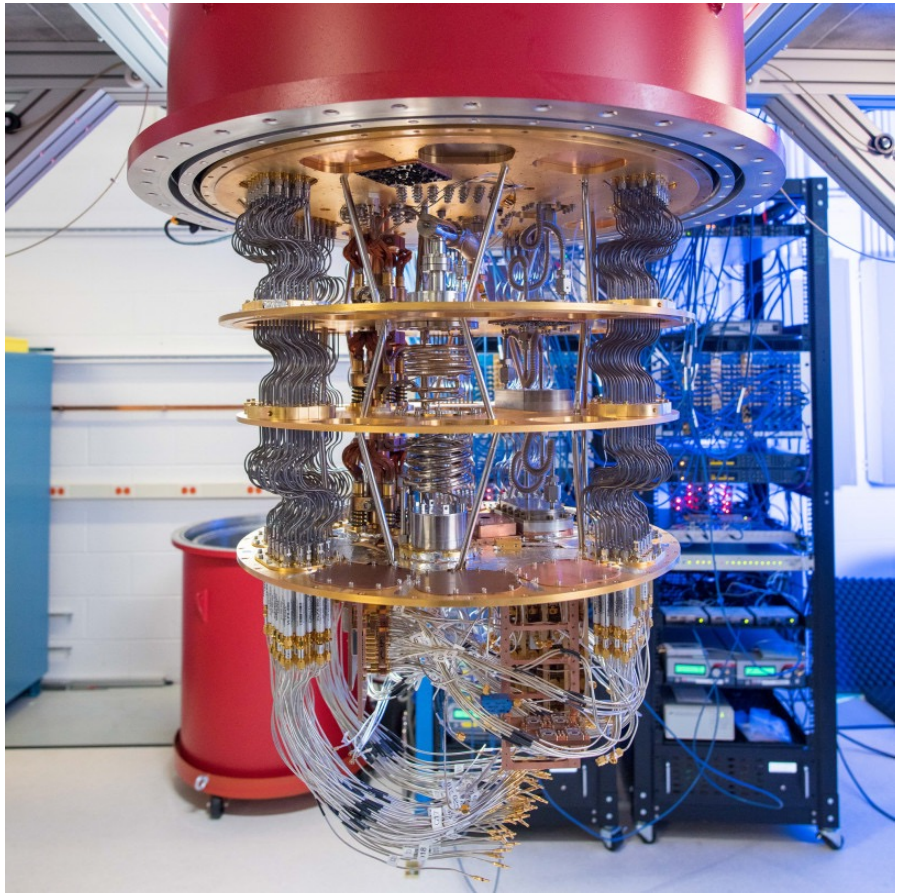
There is no easy way to find m and n before the quantum computer.

https://www.ruanyifeng.com/blog/2013/07/rsa_algorithm_part_two.html

Shor algorithm by Quantum computer

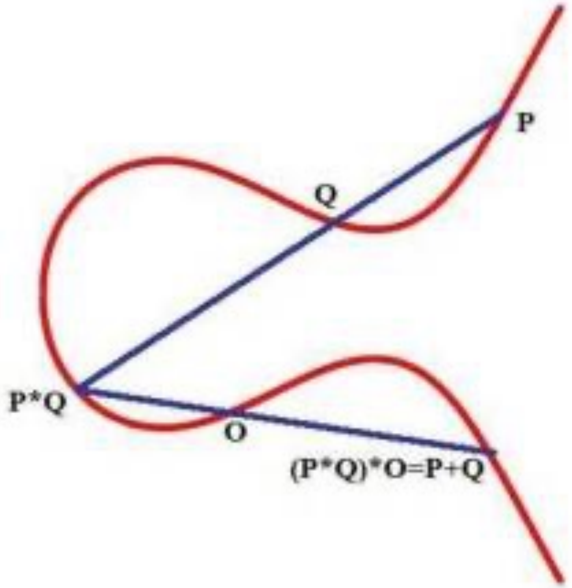
$$
\begin{aligned}
F(|\phi\rangle) = \frac{1}{\sqrt{4}}\Big[\quad & \frac{1}{\sqrt{8}}\left(|0\rangle + e^{i\frac{2\pi}{8}1}|1\rangle + e^{i\frac{2\pi}{8}2}|2\rangle + e^{i\frac{2\pi}{8}7}|7\rangle\right) \\
& + \frac{1}{\sqrt{8}}\left(|0\rangle + e^{i\frac{2\pi 3}{8}1}|1\rangle + e^{i\frac{2\pi 3}{8}2}|2\rangle + e^{i\frac{2\pi 3}{8}7}|7\rangle\right) \\
& + \frac{1}{\sqrt{8}}\left(|0\rangle + e^{i\frac{2\pi 5}{8}1}|1\rangle + e^{i\frac{2\pi 5}{8}2}|2\rangle + e^{i\frac{2\pi 5}{8}7}|7\rangle\right) \\
& + \frac{1}{\sqrt{8}}\left(|0\rangle + e^{i\frac{2\pi 7}{8}1}|1\rangle + e^{i\frac{2\pi 7}{8}2}|2\rangle + e^{i\frac{2\pi 7}{8}7}|7\rangle\right)\Big]
\end{aligned}
$$

- So far, the public reported maximum number is 21.



https://zhuanlan.zhihu.com/p/139329165

ECC: Elliptic Curve Cryptography



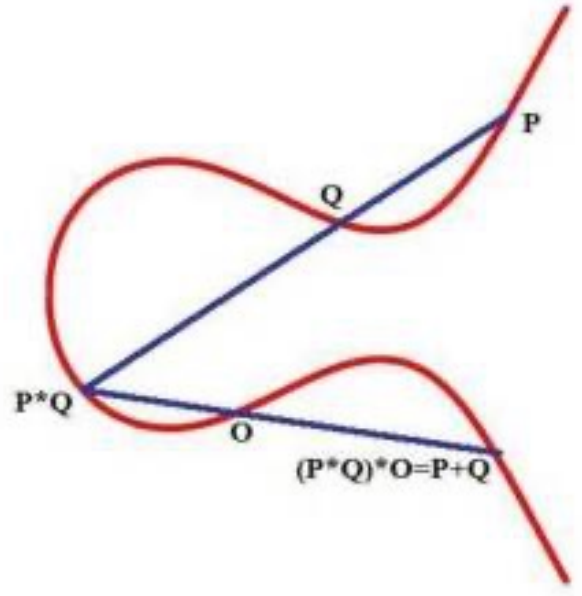
$$y^2 = x^3 + ax + b$$

对比项目	ECC 加密算法	RSA加密算法
密钥长度	256位	2048位
CPU占用	较少	较高
内存占用	较少	较高
网络消耗	较低	较高
加密效率	较高	一般
破解难度	具有数学特性，破解难度大	难破解，但相对ECC理论上容易一些。
抗攻击性	强	一般
可扩展性	强（密钥长度较短，具有更好的扩展空间）	一般
兼容范围	新版浏览器和操作系统均支持，但存在少数不支持的平台，例如cPanel。	广泛支持

- Much more complex math theory.
- Relative short key to achieve the same security.
- up-to-date application prefer ECC. Blockchains like Bitcoin using ECC encryption.

https://www.zhihu.com/question/29549792

ECC: Elliptic Curve Cryptography



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

secp256k1标准曲线的领域参数如下：

```
p = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEFFFFFC2F
a = 0
b = 7
xG = 0x79BE667EF9DCBBAC55A06295CE870B07029BFCDB2DCE28D959F2815B16F81798
yG = 0x483ADA7726A3C4655DA4FBFC0E1108A8FD17B448A68554199C47D08FFB10D4B8
n = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFEBAAEDCE6AF48A03BBFD25E8CD0364141
h = 1
```

- Much more complex math theory.
- Up-to-date application prefer ECC.
- Blockchains like Bitcoin using ECC encryption.

https://www.zhihu.com/question/29549792

Chinese algorithms of asymmetric encryption

国家密码管理局

WWW.SCA.GOV.CN

SM2标准椭圆曲线叫做sm2p256v1，具体领域参数如下：

```
p = 0xFFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFF
a = 0xFFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00000000FFFFFFFFFFFFFFFC
b = 0x28E9FA9E9D9F5E344D5A9E4BCF6509A7F39789F515AB8F92DDBCBD414D940E93
xG = 0x32C4AE2C1F1981195F9904466A39C9948FE30BBFF2660BE1715A4589334C74C7
yG = 0xBC3736A2F4F6779C59BDCEE36B692153D0A9877CC62A474002DF32E52139F0A0
n = 0xFFFFFFFEFFFFFFFFFFFFFFFFFFFFFFFF7203DF6B21C6052B53BBF40939D54123
h = 1
```

- SM3 is an ECC with a group of specific parameters

https://www.jianshu.com/p/5b04b66a55a1

Short summary of Symmetric and Asymmetric

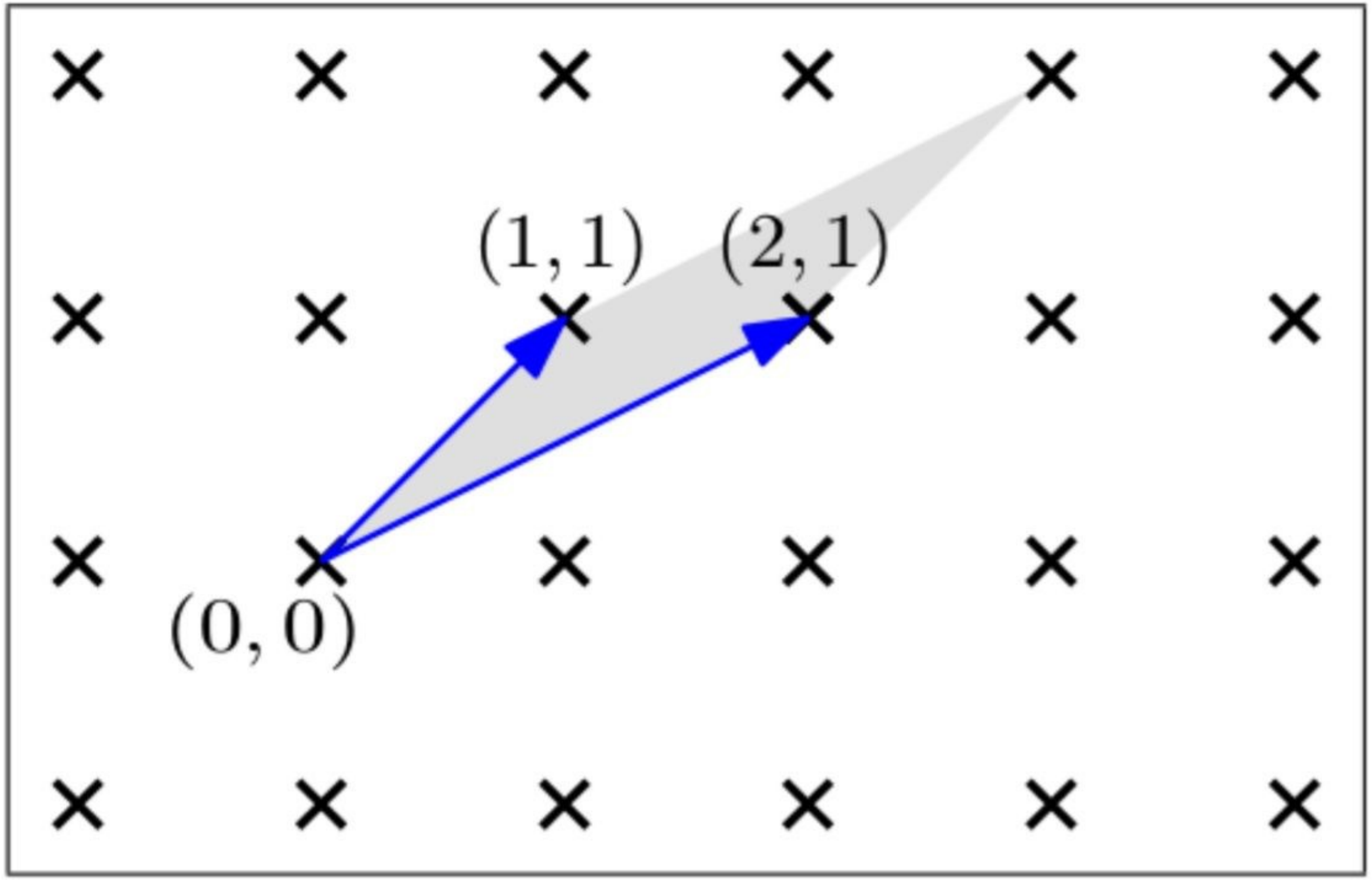
Table 1. Security Comparison for Various Algorithm-key Size Combinations (Source: NSA) [7]

Security Bits	Symmetric Encryption Algorithm	Minimum Size (bits) of Public Keys	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

- **The security of different algorithms CANNOT be compared directly.**
- **Maybe surprise, with the same length of key, symmetric encryption IS more safe than asymmetric one.**
- **The No.1 challenge of symmetric encryption is how to SHARE the keys between Alice and Bob.**
- **All keys CAN be broken. The main issue is about "money", does is worth to be broken?**
- **New technology may make certain algorithm no longer secure.**
- **One good application always combines the advantages of different algorithms.**

https://www.netburner.com/learn/comparing-rsa-and-ecc-encryption/

One more thing: Lattice encryption



(b) Another basis of $\mathbb{Z}^2$

https://zhuanlan.zhihu.com/p/222217422