Fun with cryptography

Frank Fu

Dalhousie University

Feb 24, 2021

The age of internet

Common questions

- How to ensure our communication is secure?
- How to make sure the website is legitimate?

Encryption

Figure 1: Symmetric encryption.

Caesar cipher

An example:

- A → C, B → D, C → E, ..., X → Z, Y → A, Z → B
- key: 2
- How to encrypt “MAGIC”?

Math with 26 numbers : $\{0, 1, 2, \ldots, 25\}$

- $10 \oplus_{26} 7 = 17$
- $1 \oplus_{26} 25 = 0$
- $10 \oplus_{26} 17 = 1$
- $10 \ominus_{26} 7 = 3$
- $1 \ominus_{26} 25 = -24 = 26 - 24 = 2$

Math behind Caesar cipher

- Encryption.

$$x \mapsto x \oplus_{26} \text{key}$$

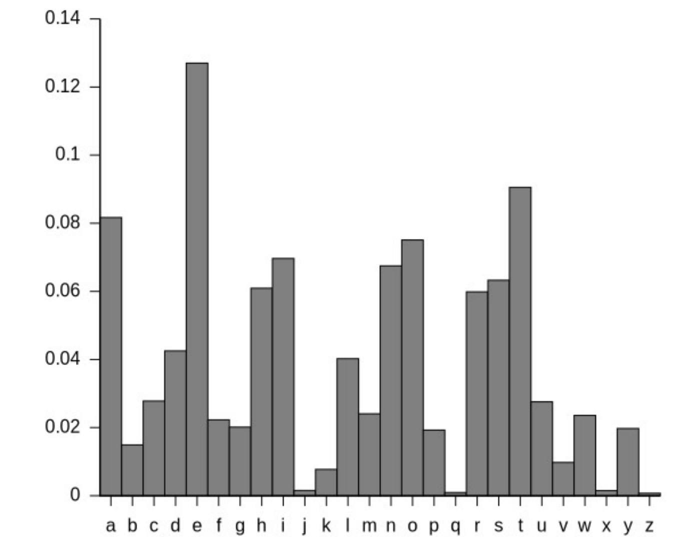
- Decryption.

$$x \mapsto x \ominus_{26} \text{key}$$

- "MAGIC" = 12, 0, 6, 8, 2

  $\mapsto$ 14, 2, 8, 10, 4 = "OCIKE"

Attack on Caesar cipher: bruce force and letter frequency



Attack on Caesar cipher

Can you decrypt "ALIIP" (= 0, 11, 8, 8, 15) ?

(A,0)	(B,1)	(C,2)	(D,3)	(E,4)	(F,5)
(G,6)	(H,7)	(I,8)	(J,9)	(K,10)	(L,11)
(M,12)	(N,13)	(O,14)	(P,15)	(Q,16)	(R,17)
(S,18)	(T,19)	(U,20)	(V,21)	(W,22)	(X,23)
(Y,24)	(Z,25)				

Attack on Caesar cipher

Can you decrypt “ALIIP” (= 0, 11, 8, 8, 15) ?

- $E = 4$.
- $4 \oplus_{26}$ key $= 8 = I$
- key $= 8 \ominus_{26} 4 = 4$
- 22, 7, 4, 4, 11 = “WHEEL”

Does the perfect cipher exist?

The perfect cipher: One Time Pad

- "MAGIC" = 12, 0, 6, 8, 2
- Encryption

  $12 \oplus_{26} \_ =$

  $0 \oplus_{26} \_ =$

  $6 \oplus_{26} \_ =$

  $8 \oplus_{26} \_ =$

  $2 \oplus_{26} \_ =$

One Time Pad

- Key must be used exactly once
- Key must be chosen randomly
- Acheive perfect secrecy
- length(Key) = length(Message)

Cryptographic protocol

- Alice and Bob has their own keys and locks.
- A box with two places for locks.
- How can Alice and Bob communicate securely?

Cryptographic protocol

An example.

- Alice and Bob has their own keys and locks.
- The lock must be open and lock by the key.
- A box with two places for locks.
- How can Alice and Bob communicate securely?

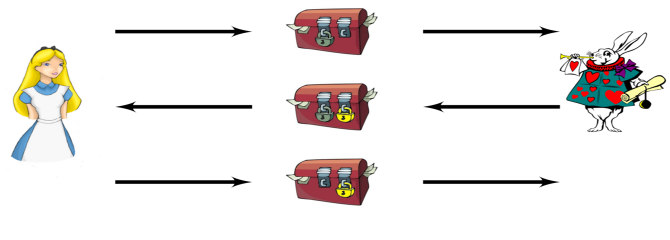


Figure 2: 3-pass Shamir protocol.

3-pass Shamir protocol

1. Alice $\longrightarrow$ Bob
   $\{m\}_a$
2. Bob $\longrightarrow$ Alice
   $\{\{m\}_a\}_b$
3. Key commutative $\{\{m\}_a\}_b = \{\{m\}_b\}_a$
4. Alice $\longrightarrow$ Bob
   $\{m\}_b$

3-pass Shamir protocol

It allows us to communicate without shared key. But.

Diffie-Hellman key exchange protocol

- Alice and Bob want to negotiate a share key.
- The negotiation can be done over an un-encrypted public channel.

Diffie-Hellman protocol in colors

Assumptions: colors are easy to mix and hard to separate.

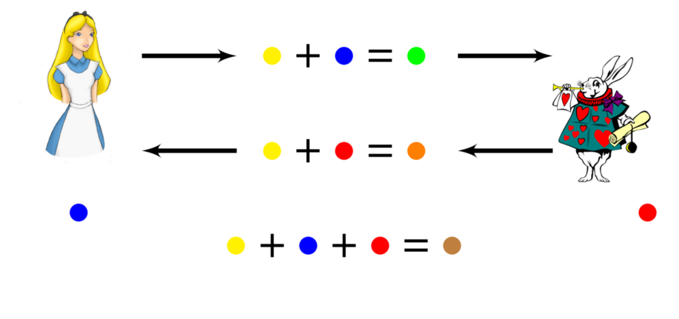


Figure 25: Diffie-Hellman protocol with colors.

Diffie-Hellman protocol in math

Given a prime p and a well-chosen number a.

- It is very easy to compute $r = a^k \pmod{p}$.
- It is very hard to compute k from r, a and p.

This is called *discrete logarithm problem*.

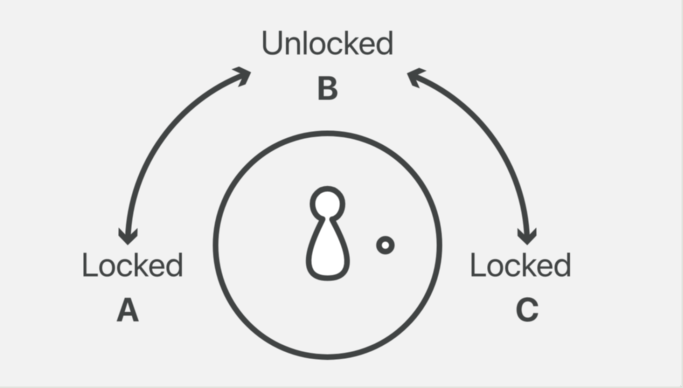
Diffie-Hellman protocol in math

1. Alice and Bob agree to use a large prime p and a special number a.
2. Alice chooses a secret integer k_1 and sends $a^{k_1} \pmod p$ to Bob.
3. Bob chooses a secret integer k_2 and sends $a^{k_2} \pmod p$ to Alice.
4. Alice computes $(a^{k_2})^{k_1} \pmod p$.
5. Bob computes $(a^{k_1})^{k_2} \pmod p$.

Note that $(a^{k_2})^{k_1} = (a^{k_1})^{k_2}$.

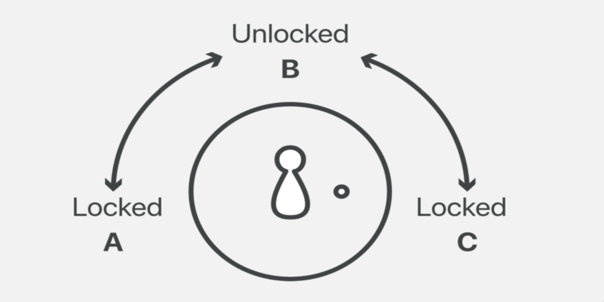
Public key protocol using a special locker

- Private key can only turn to the left
- Public key can only turn to the right



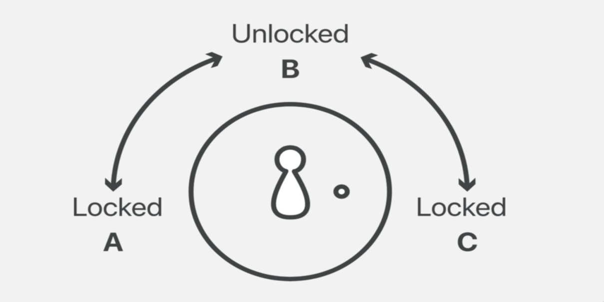
Public key protocol using a special locker

- Private key can only turn to the left
- Public key can only turn to the right
- Alice makes a few dozen copies of public key
- Alice shares public key to everyone
- Alice keeps private key to herself



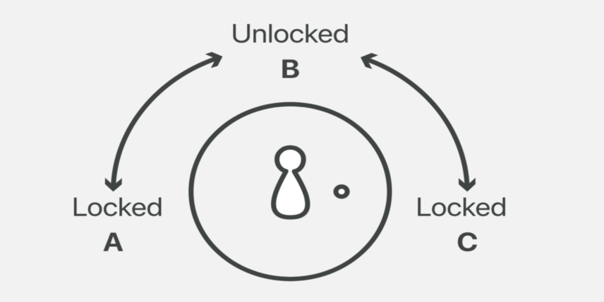
How to send a message to Alice?

- Private key can only turn to the left
- Public key can only turn to the right

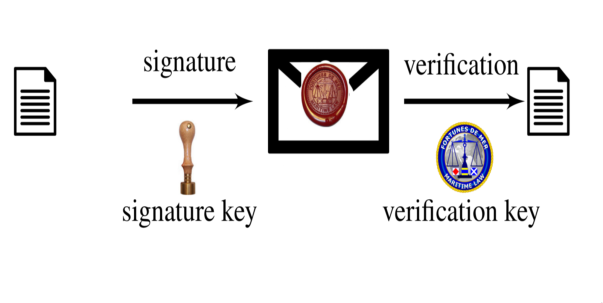


Can we be sure a message is from Alice?

- Private key can only turn to the left
- Public key can only turn to the right



Digital signature



Public key protocol

- Public key protocol support both encryption and digital signature.
- Today the most commonly used public key protocol is called RSA.
- It is named after Ron Rivest, Adi Shamir and Leonard Adleman.
- It is also the first public key encryption scheme.

Conclusion

- We learned Caesar's cipher and the perfect One Time Pad.
- We learned about 3-pass Shamir protocol.
- We learned about Diffie-Hellman key exchange protocol.
- We learned about the basic of Public key protocol.

References

- *How to Explain Modern Security Concepts to your Children*, Xavier Bultel, Jannik Dreier, Pascal Lafourcade, Malika More
- *How Does Public Key Encryption Work*? `https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/`