CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

Cryptography All-in-One, a full introduction

- Why is Cryptography essential?
- What is Cryptography
  - How does cryptography work?
- Applications of Cryptography
- Types of Encryption in Cryptography
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography
- Hashing (TBD, in Part3)
- Data Encryption Standard (DES) Algorithm (TBD, in Part3)
- Advanced Encryption Standard (AES) Algorithm (TBD, in Part3)

Cryptography All-in-One, a full introduction

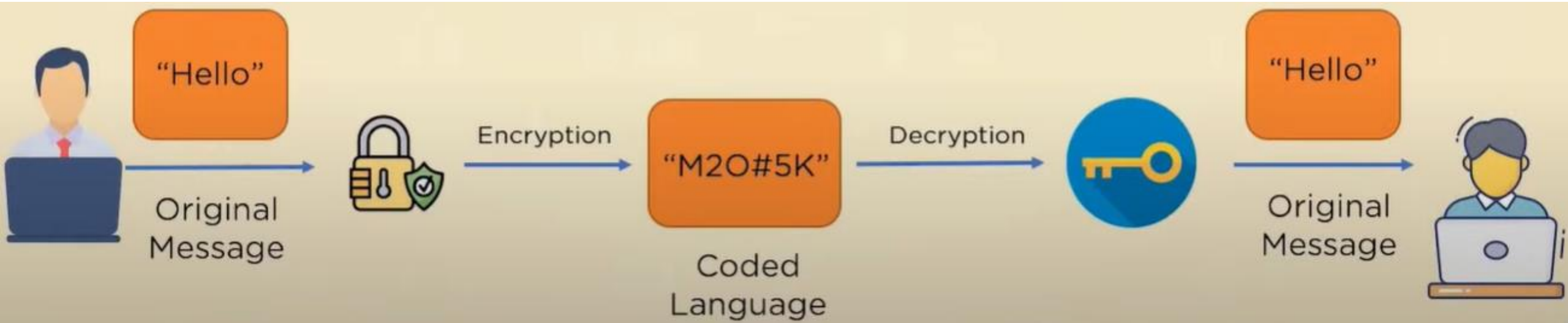
- Digital Signatures Algorithm (DSA) (TBD, in Part3)
- Rivest-Shamir-Adleman Encryption (RSA) (TBD, in Part3)
- Message Digest – 5 (MD5) Algorithm (TBD, in Part3)
- Secure Hash Algorithm (SHA) (TBD, in Part3)
- Secure Socket Layer (SSL) Handshake (TBD, in Part3)
- Diffie-Hellman Key Exchange (TBD, in Part3)

Why is Cryptography essential?

- In one sentence: Cryptography can help to send the data, receive the data and store the data safely.
- Think about the following scenario.
  - If we go to a commercial website to purchase something, and this website is unfortunately a http instead of a https (in the browser address line)
  - The product you clicked
  - The name and address you setup as a receiver's info.
  - The credit card number, exp. date and the security code is totally viewable by
    - Website owner
    - Hacker (you don't know if the website has infected with Trojan or worms)
    - Any unrelated person.

What is Cryptography

- Cryptography is the science of encrypting and decrypting information to prevent unauthorized access.
- The **decryption** process should be known to both the sender and the receiver
  - The ways for encryption? It is not necessarily to be known by receiver



How does cryptography work?

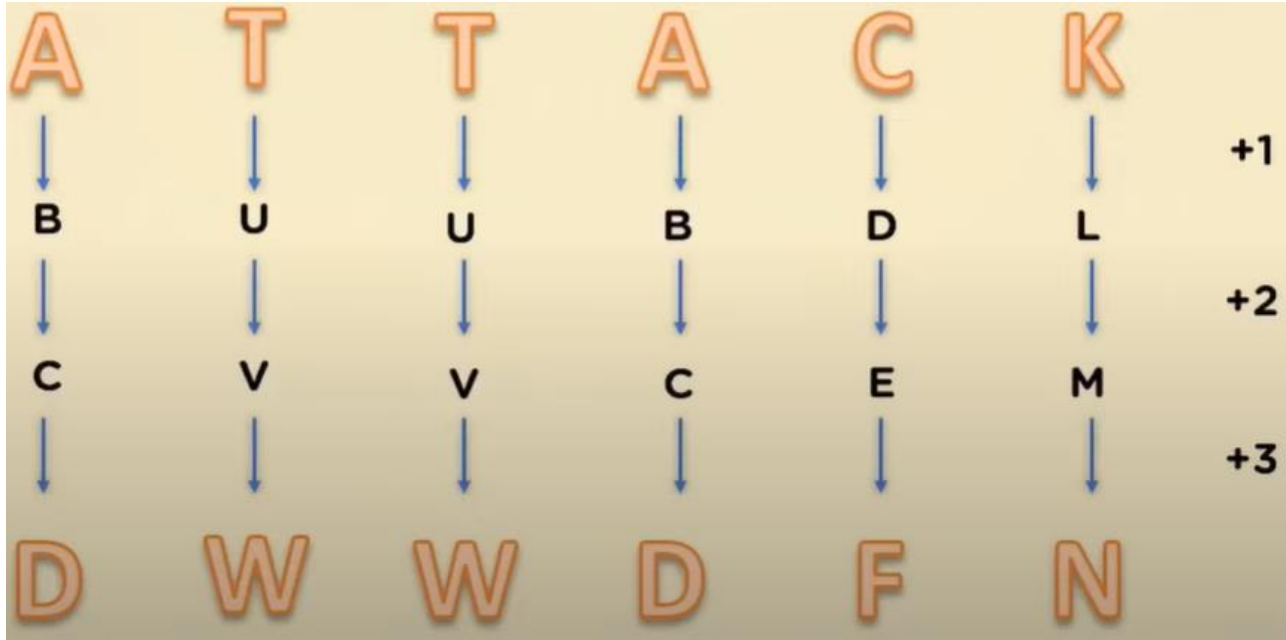
- For encryptions, we need algorithms to chop and mix the data
- The decryption is nothing but to make the data readable again

How does cryptography work?

- Here is an example, a very ancient but is still an useful trick.
- For example, the input string is “Charles”
- If there is an encryption algorithm: **exchanging the alphabet with the next one**
- The output string will be: “Hcraels”
- Now we send out the encrypted string “Hcraels”
- Then, the next job is to make sure the receiver knows the algorithm, so he can do the decryption and see the original string.

How does cryptography work?

- Another ancient example, the “Caesar cipher”
  - Used by Julius Caesar in thousands years ago
  - He use this to transfer messages between his armies
  - Alphabets are moved by a certain number
  - For example, if the shift is 1, A becomes B, B becomes C and so on.
  - If we choose “+3”, then it will be “DWWDFN” compared with our original plaintext “ATTACK”



Applications of Cryptography

- The new booming crypto-currency is a good example.
- Cryptography is not limited to the encrypted emails

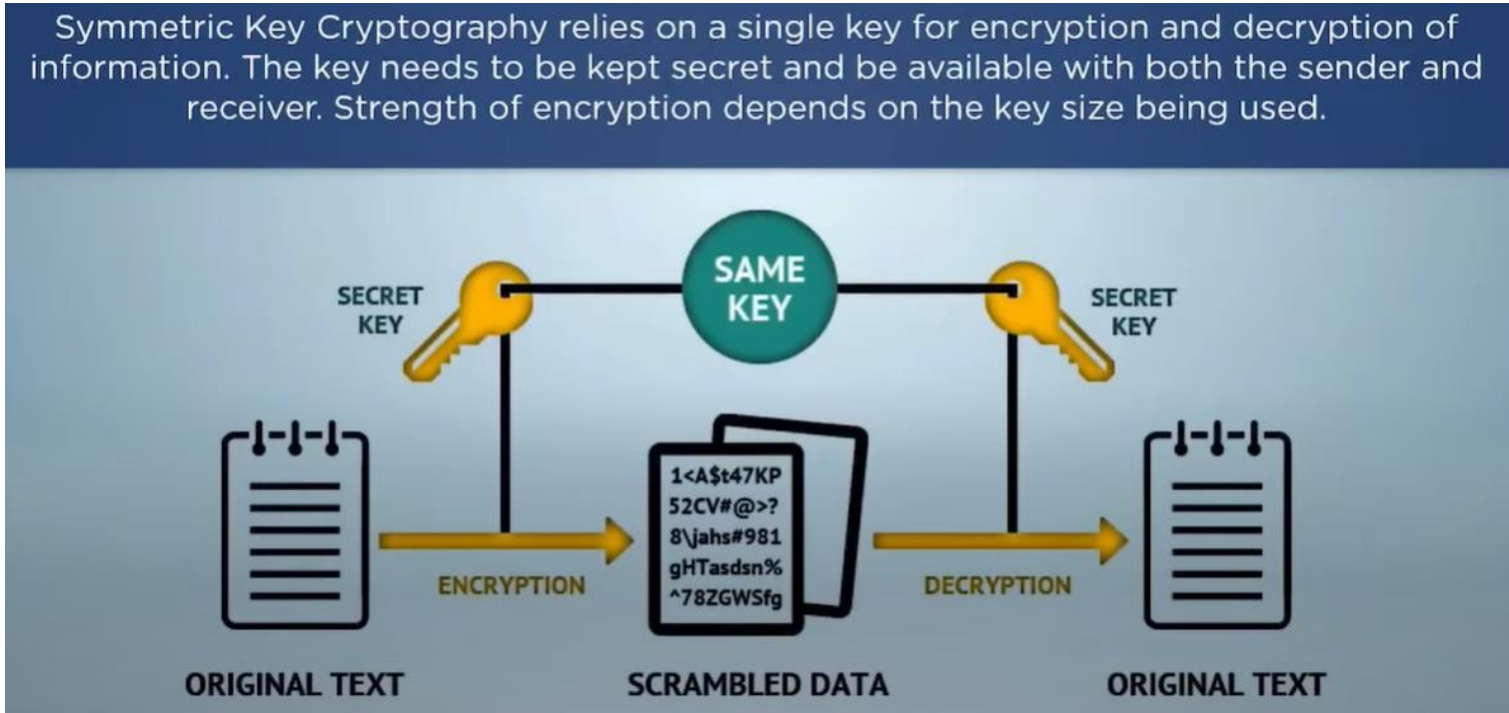
Types of Encryption in Cryptography

- For the 2 types of cryptography, they only differs in its implementation

Symmetric Key Cryptography

- The point is, the key has to be pre-shared!
- The strength of encryption depends on the key size (length) is chosen.
- But the point is, how to keep the key being private? There is only public key!
- If someone intercepts

the key and also intercepts the cipher text as well, he can know the plain text with a decryption on the fly

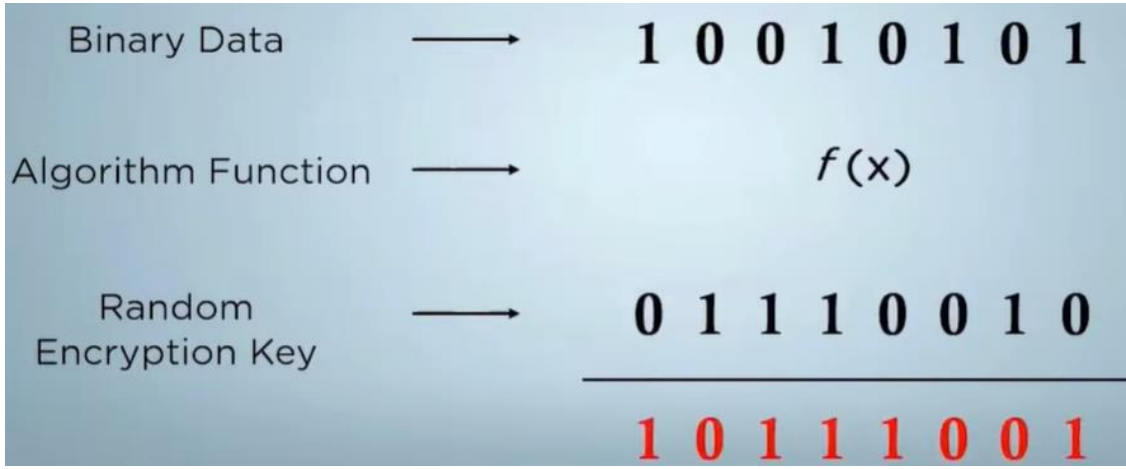


Symmetric Key Cryptography

- In Symmetric Key Cryptography, there are 2 categories of ciphers that we can employ.
  - **Stream ciphers:** Some algorithms that encode basic information **one bit at a time**.
    - It can change depending on the algorithm being used but usually, it relies on a single bit or byte to do the encryption
    - Data is converted into binary format (first step) and encrypted (second step) sequentially.
    - The most popular ones are rc4, salsa and panama

Symmetric Key Cryptography

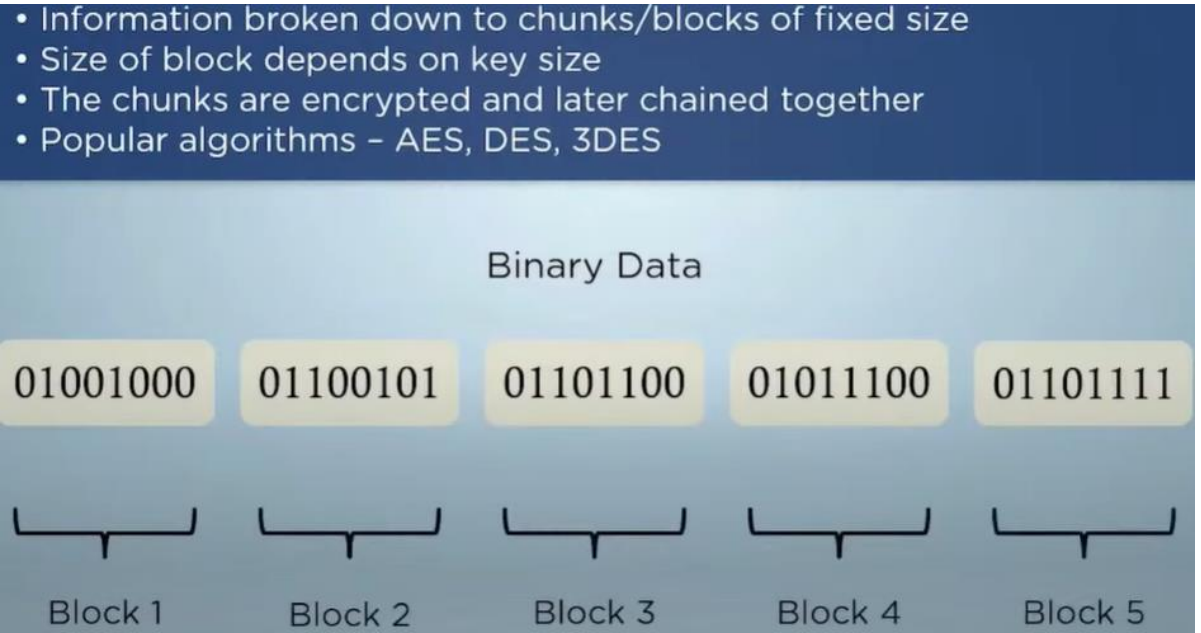
- Let's take a look at a simple example, the XOR operation
- The **plain text** is converted in **binary format**
- The **encryption key is randomly generated** with a **fixed length**
- Algorithm function is the XOR operation
- Here is the output for our ciphertext

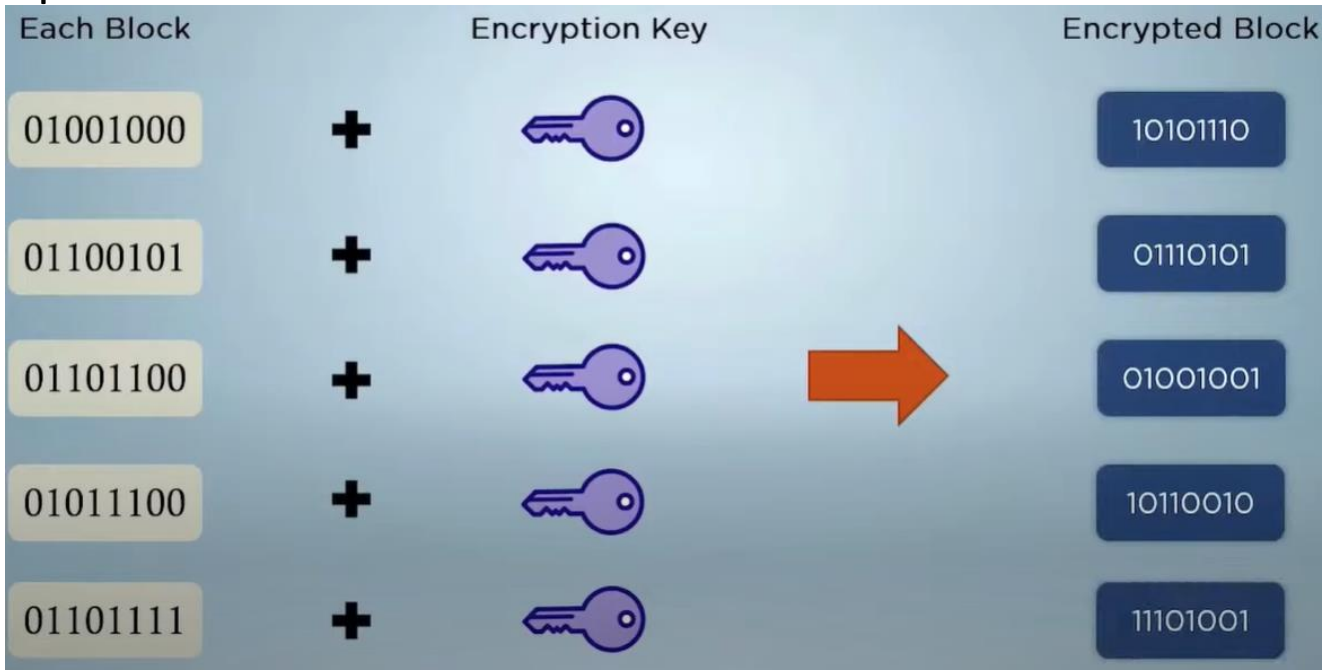


- **Block ciphers:**
  - The info. is broken down into **blocks** of fixed Size
  - The **size** of these blocks depend on the exact cipher being used.
  - For example, a 128-bit block cipher will break the plain text into blocks of 128 bit each and encrypt those blocks instead of a single digit
  - Once these blocks are encrypted individually, they are **chained together** to form a final cipher text

Symmetric Key Cryptography

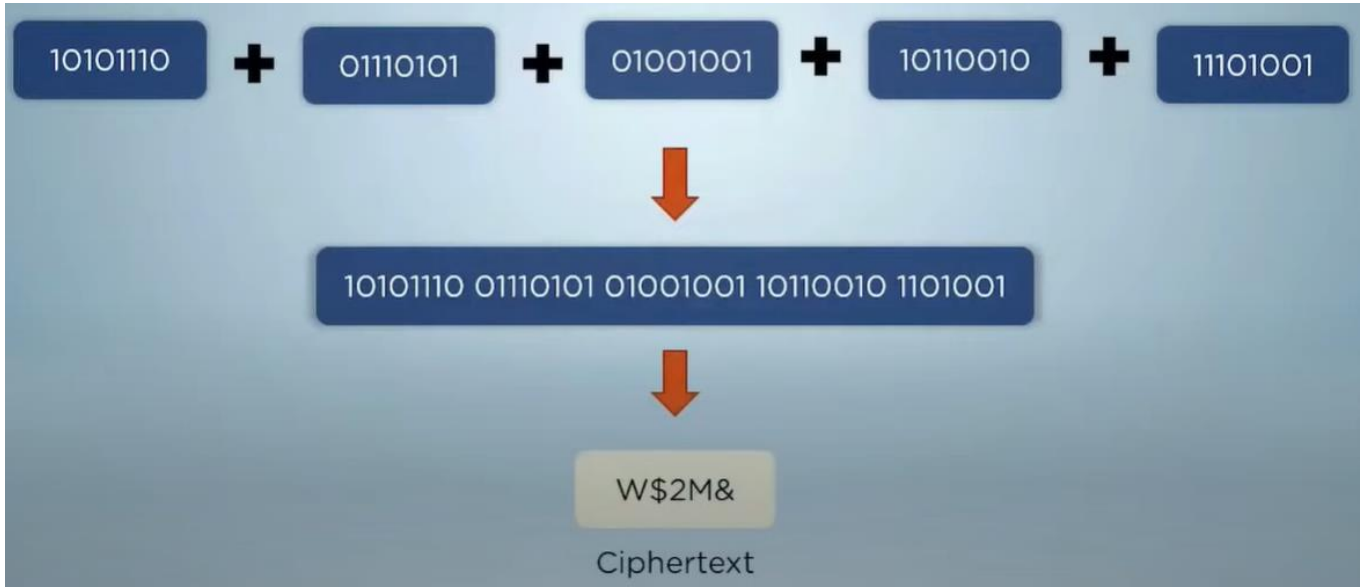
- Block cipher are much **slower** but they are more tamper-proof and are used in some pf the most widely used algorithms employed today
- Like stream ciphers, the original data is converted in binary format
- Once the conversion is complete, the blocks are passed through the encryption algorithm, along with the encryption key → yield the encrypted blocks
- So, those are the properties of Block Ciphers





Symmetric Key Cryptography

- Once these blocks are combined, we get a final binary string. So the string is then converted into hex format (optional) to get out cipher text
- AES, DES, 3DES (most popular ones) are **all** block cipher methodology
- **Advantages?**
  - Faster than asymmetric cryptography (encryption and decryption)
  - Only one key is in the play



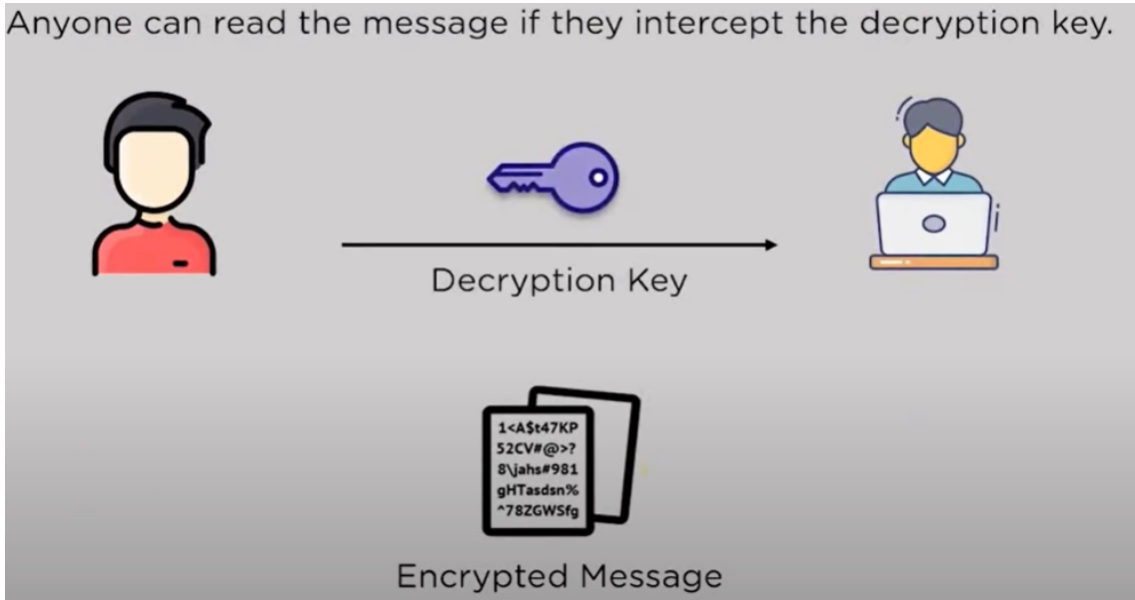
Asymmetric Key Cryptography

- Assuming there are 2 persons, Joe (in red color) and Ryan
- Since Symmetric Key Cryptography is using the same key for encryption and decryption, there is a problem. How does Joe send the decryption key to Ryan?
- The truth is, the key might get intercepted!
- Key sharing is risky when symmetric

cryptography is being used

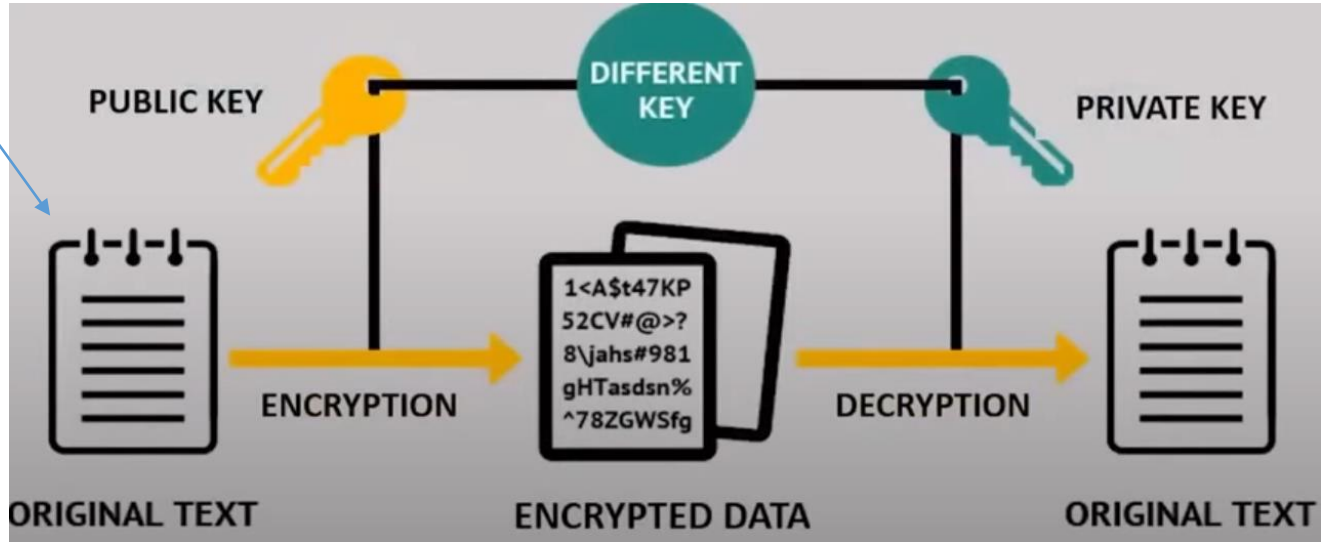
- Solution? Asymmetric Key

Cryptography!



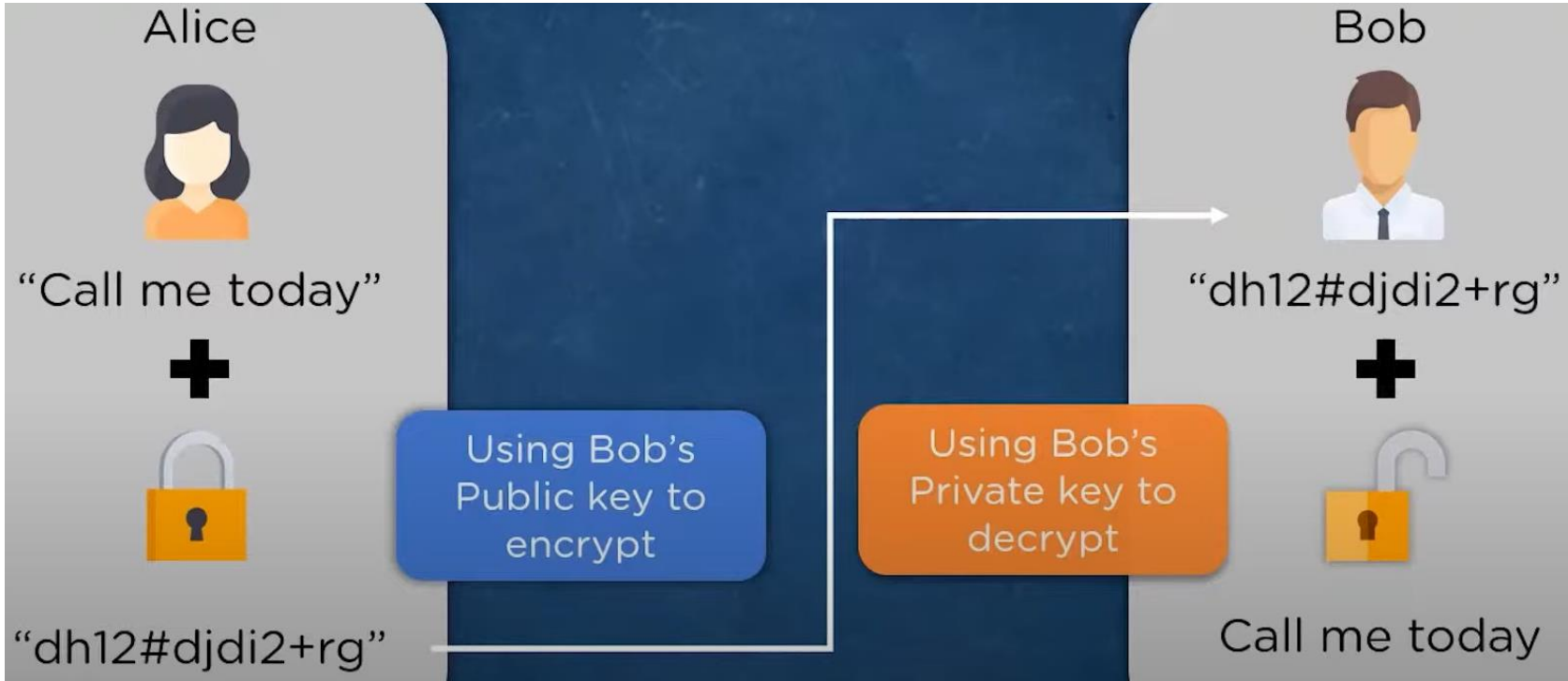
Asymmetric Key Cryptography

- Encryption: public key
- Decryption: private key
- The public key can be shared with messaging, blog posts (dangerous), or key servers, before the data transfer.
- So, from this picture, the sender, must get receiver's public key before file / data transfer begins.
- No key exchanges in the data transfers but key exchanges happens in the earlier stage



Asymmetric Key Cryptography

- Here is an example.
- When Bob get the message from Alice, it the beginning, it is just a “dh12#djdi2+rg”
- He needs to use his own private key to decrypt it



Asymmetric Key Cryptography

- Any applications in Asymmetric Key Cryptography?
  - Digital Signatures (introduced in our previous lecture)
    - Private key to sign the message to guarantee the authenticity (like the blood has DNA in it)
    - Hash is like the seal of the letters, to guarantee the message is not tampered (opened)
    - Receiver can use the public key to verify the signature
    - Since the public key and private key in the signature is linked mathematically, it is impossible to repeat (to fake) this verification with duplicate keys
  - Crypto currency transactions
    - The transaction has to be managed
    - The transaction is happened, “only if” it is approved from both ends in the peer-to-peer network
    - Tamper-proof

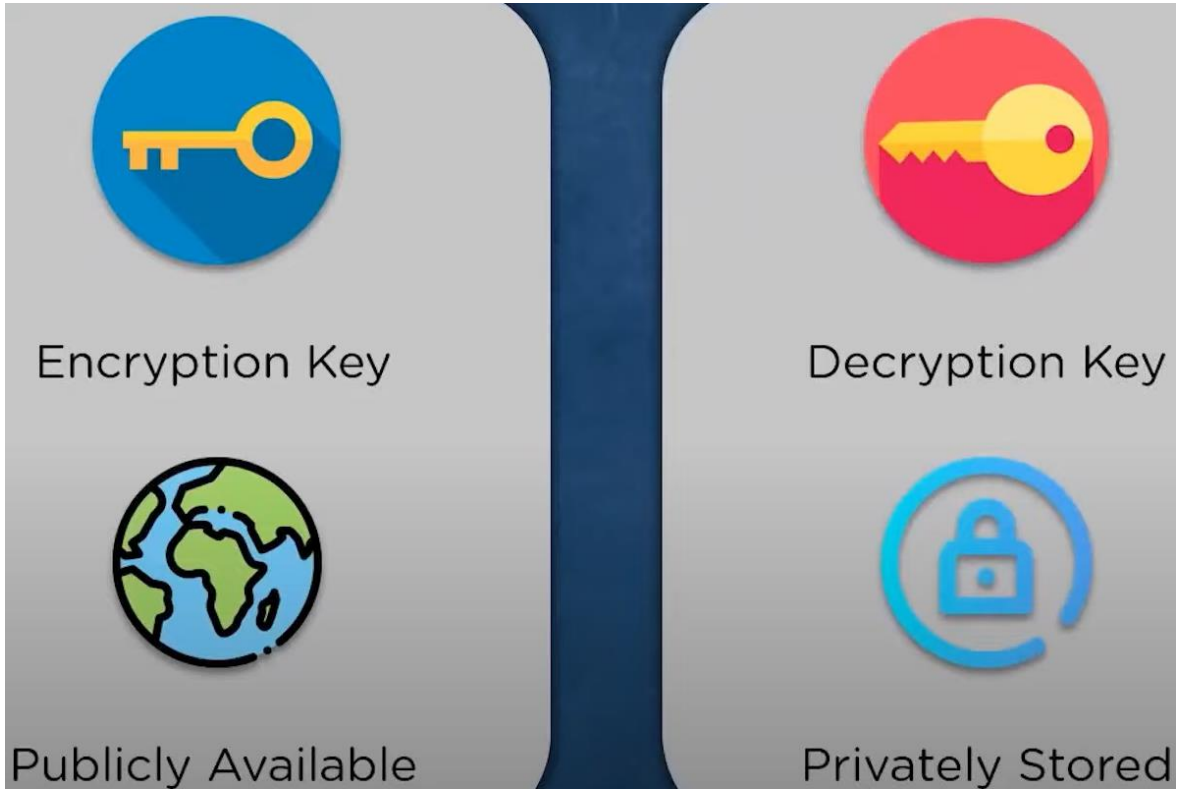
Asymmetric Key Cryptography

- Encrypted browsing
  - i.e. SSL connections

Asymmetric Key Cryptography

- There is a silly question what can always challenge your mind.
  - Why asymmetric cryptography is called public key cryptography?

  Answer:



- Oh! Oh! Oh! You will have a 5% homework for this cryptography
  - The good news is, it will be very easy.
  - No programming
  - There is only Q&A
  - Everything is in the slides ☺