Encryption

Encryption is the process of scrambling data in such a way that only legitimate users can read it.

- Converts Plaintext to Ciphertext
- Symmetric Key encryption
- Asymmetric Key Encryption

Symmetric Encryption

- The same key is used for both encryption and decryption
- must be long enough that it becomes infeasible for a normal sized computer to crack the encrypted message in a reasonable amount of time
- AES-256 (Advanced Encryption Standard - 256 bits)
  - standard algorithm used by national governments and commercial organisations

Caesar Cypher

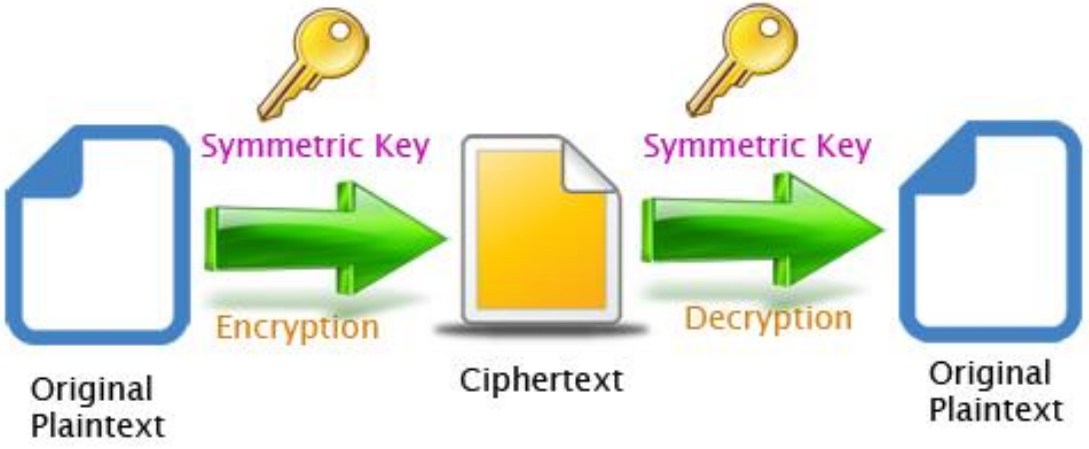
- Used by Roman Emperor Julius Caesar
- Very simple and easily cracked
- Letters are swap for another letter an agreed number of positions up in the alphabet

Book Cypher

- Not practical for long messages!
- Two parties agree to use a certain book.
- The message is created by referencing a letter or word in various pages within the book.
- For example the code might be 724. Meaning use the 72th letter on page 4.
- Relies on knowing which book is being used

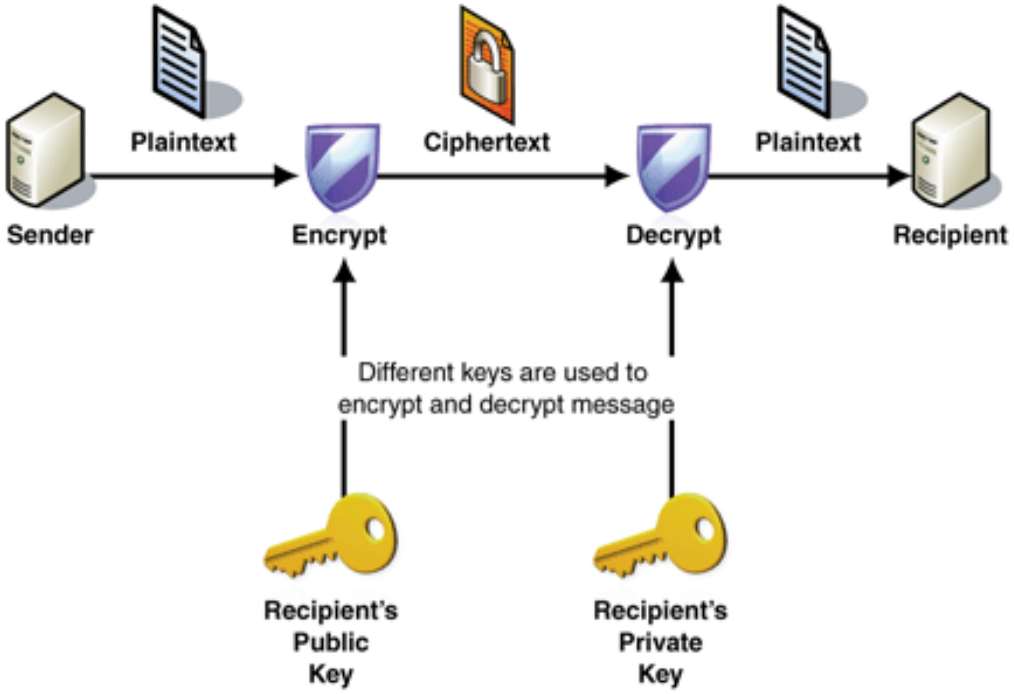
Symmetric

- Needs the key to be kept secret
- Keys can be calculated using time for it to change regularly
- Process is called “exchanging the key”
- Need key exchange algorithm (SSL/TLS)



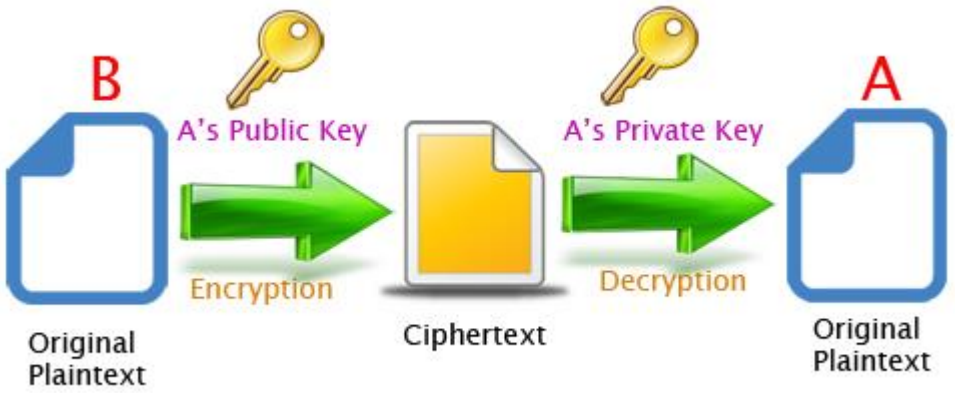
Asymmetric Encryption

- Cannot send symmetric key over net (as its plain text)
- Different keys used to encrypt and decrypt
- Called Key pair



Asymmetric Encryption

- Used by digital signatures
- British concept – GCHQ 1970
- Implemented in 1973
- Public available in 1976
- Eliminates man in the middle attacks



Symmetric v/s Asymmetric

Characteristic	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for encryption / decryption	Same key is used for encryption and decryption	One key used for encryption and another, different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than the original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks)

- https://en.wikibooks.org/wiki/Cryptography/A_Basic_Public_Key_Example
- https://www.youtube.com/watch?v=YEBfamv-_do
- https://www.youtube.com/watch?v=AQDCe585Lnc
- https://www.youtube.com/watch?v=56fa8Jz-FQQ

Hashing

- Hashing is a method of cryptography that converts any form of data into a unique string of text
- Traditionally hashing of any data (regardless of the data's size, type, or length) generates a hash that is always the same length
- A unique piece of data will always produce the same hash.

Hashing

- Hashing is a mathematical operation
- Easy to perform
- Extremely difficult to reverse
- The difference between hashing and encryption is that encryption can be reversed, or decrypted, using a specific key.

Hashing Uses

- ISP will store your password as a hash
- Your password is put through a hashing algorithm and the hash is stored
- When you sign in your password is encrypted and the hash is compared

Hashing Tools

- http://onlinemd5.com
- http://www.sha1-online.com

Salting

- Salting includes adding random data to a password before hashing it
- The ‘salt value’ is stored with the hash
- Makes decrypting much much harder

- https://www.youtube.com/watch?v=cczlpiiu42M