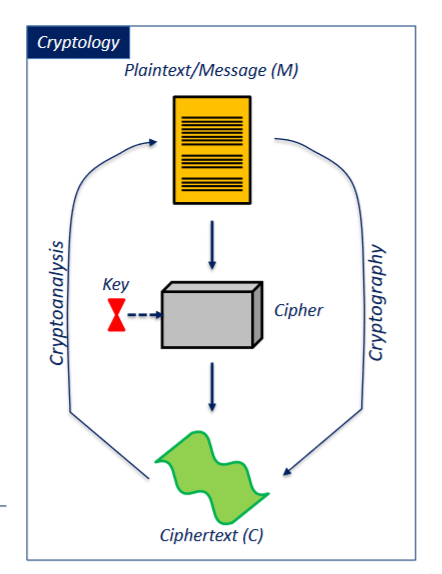
Intro to Cryptography

Terminology

* Plaintext / Message: readable message
* Cipher: cryptographic algorithm
* Ciphertext: message after cipher
* Cryptography: constructing and analysing encryption
* Cryptoanalysis: gain access to the contents of encrypted messages, even if the cipher is unknown
* Cryptology: Cryptography and Cryptoanalysis together

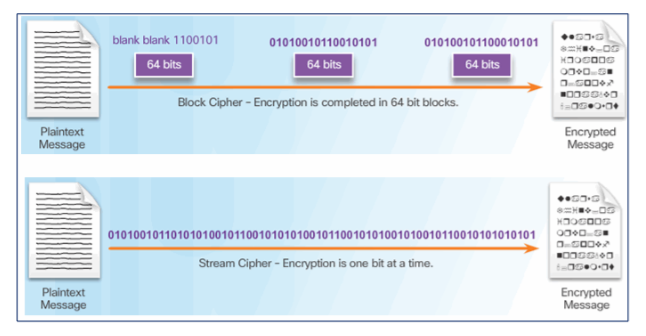
Relationship between words in terminology

More terminology

* Key space: each cipher has it; a range from which the keys must come
* Key size / length: length of keys in bits n; keys can be numbers from 0 … 2^(n), e.g., 128-bit key has values from 0 … 2^(128)
* Rounds: a cryptographic system (software) might apply a certain cipher to a message several times

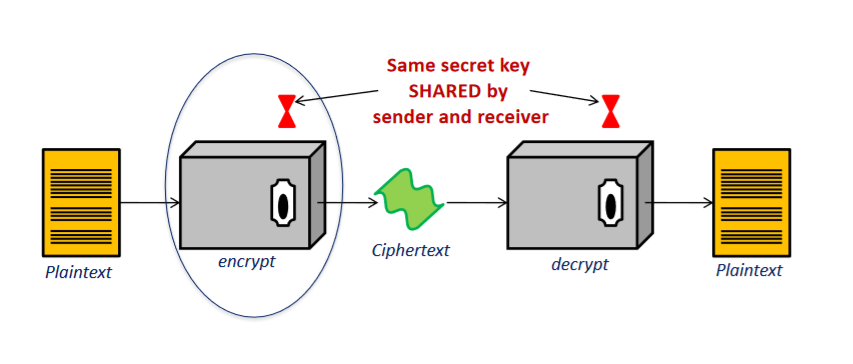
2 Types of cipher

* Block cipher: splits a message into blocks of a certain block size (in bits) and encrypts per block
* Stream cipher: encrypts bit per bit, so it does not have a block size

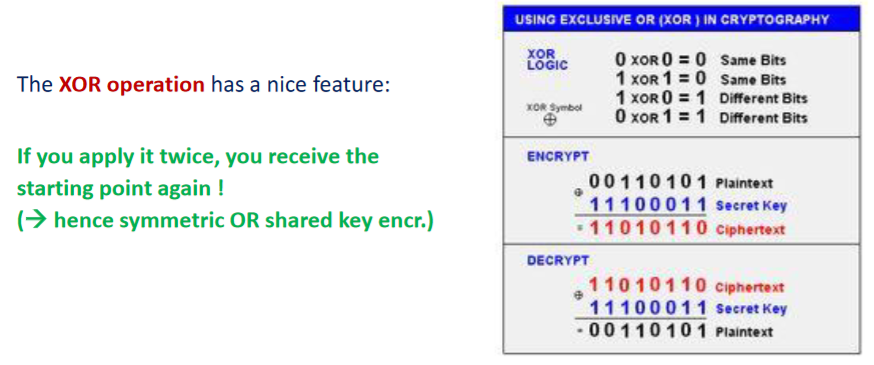


Symmetric Encryption

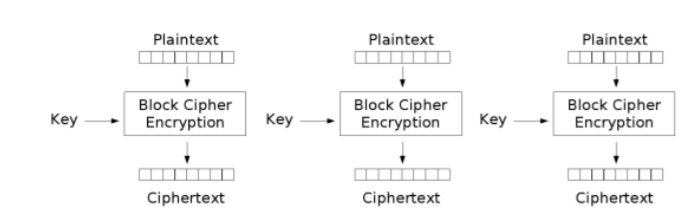
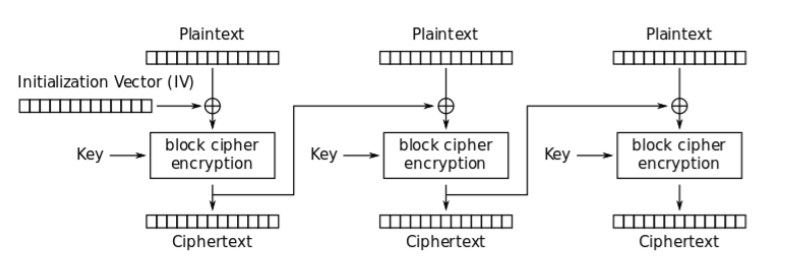
Principle of symmetric encryption



Mathematical foundation of symmetric encryption



Variants of symmetric encryption

* Electronic Codebook mode
  + Simplest form of symmetric encryption
  + Encryption block by block
* Cipher Block Chaining
  + More advanced
  + Makes use of the first block’s ciphertext for encrypting the next block

Advantages and Problems of symmetric encryption

Both sides have to keep the shared key secret (hence the name “private key encryption”)

Problems:

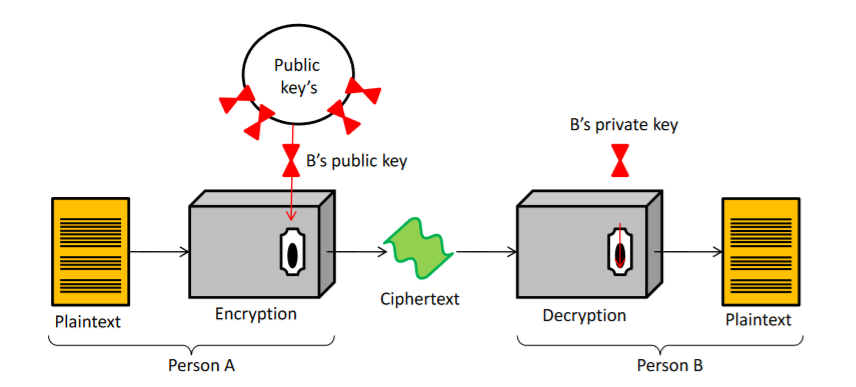
* Key distribution is difficult; parties must have a secure channel to share the key
* Non-repudiation: (= impossibility to deny authorship) is NOT given
* Algorithm is not scalable to a larger group than two people
* Keys must be detected and regenerated often, e.g., always when someone leaves a group or a key has become open

Advantages:

* Fast to compute (XOR)

Asymmetric encryption

Principle of asymmetric encryption



Example for mathematical foundation of asymmetric encryption

The RSA (Rivest-Shamir-Adlemen) public key algorithm, one of the most used algorithms, is based on prime numbers and the module operation:

1. Choose two large prime numbers p and q
2. n = p \* q and m = (p-1) \* (q-1)
3. Select a number e < n such that e and m are relative primes (= do not have factors in common other than 1)
4. Find a number d such that (e \* d – 1) mod m = 1
5. Distribute (e, n) as public key and keep (d, n) as private key

Use public key to encrypt plain message P; C = P^(e) mod n

Use private key to decrypt ciphertext C; P = C^(d) mod n

Example:

1. p = 17, q = 11
2. n = 187, m = 160
3. e = 7
4. d = 23

🡪 public key: P^7 mod 187

🡪 private key: C^23 mod 187

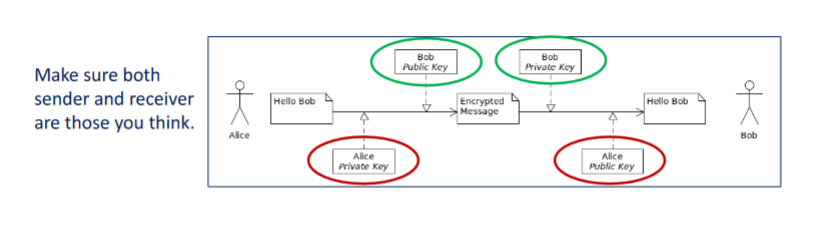
Advantages and problems of asymmetric encryption

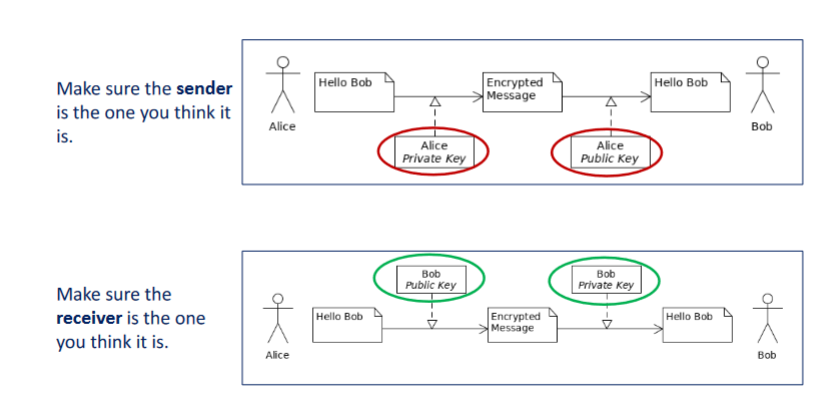
Problems:

* Slower than symmetric encryption
* Distribution of public key part: how do I get it?
* Keys have to be longer than with symmetric encryption to gain the same level of security

Advantages:

* Does not require sharing of private keys
* Nobody except the owner of a private key can decrypt a message
* With use of the private key, non-repudiation is given (when the owner of the private key has sent a message using, among others, their own private key)

Symmetric vs Asymmetric: when to use what



Hashing

Definition

A Cryptographic Hash Algorithm maps data of arbitrary size to a bit string of fixed size called Hash in a way that there is no way back

* Deterministic, i.e., always same result for same output
* Uniform, i.e., distributes hashes over whole result set
* Fast to compute
* Cannot be reversed

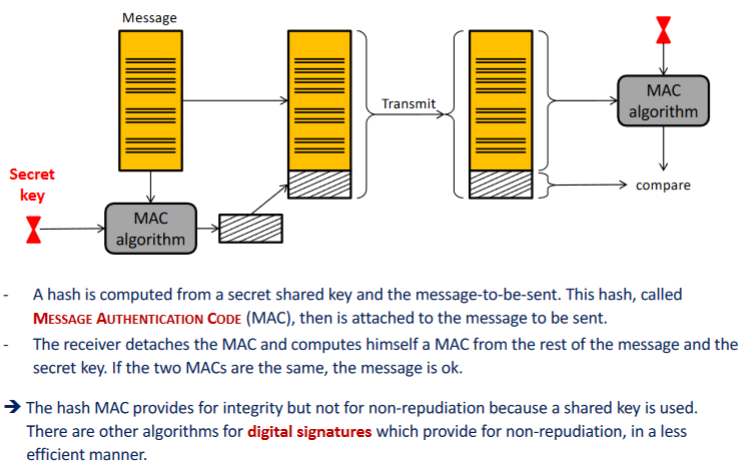
Variants

* Plain: hashing table being smaller than input data set
* Perfect match: both set of to-be-hashed and the set of hashes of the same size
* Salted: combined with another individual input, stored separately from the hash and usually changed regularly

Usage

* Rapid data lookup, for e.g., passwords in database
* Detect duplicate parts much faster
* As digital signature for a message

Hashing as a Signature

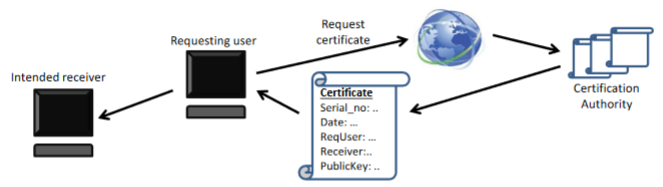


Digital Certificates

Definition

* Package of information, delivered by certification authority
* Contains: identification of requesting user, information about intended receiver, intended receiver’s public key

Process

* User requests a certificate to open a secure connection to some receiver
* Certification authority returns a certificate
* User extracts public key from certificate and can encrypt messages, so that they can be decrypted by the specific receiver only

Public Key Infrastructure

* In asymmetric encryption: enables people to communicate though they do not know each other
* Problem is: how do they get to know the public key of the other one
* Digital certificates from certificate authorities helps, called public key infrastructure
* Public key infrastructure combines

1. Digital certificates, to get the public keys
2. Asymmetric encryption, to exchange the shared symmetric keys
3. Symmetric encryption, to use for exchange further on
4. Hashing, for message authentication

