Random Number Generators

True Random Number Generators

Using noise devices and such, however it is not efficient.

Pseudo Random Number Generators

Uses an algorithm or a hardware device that generates a sequence of random bits, starting from an initial value called a seed.

The seed is usually TRN.

PRN sequence repeats periodically, should be very long, and it's periodicity depends on the size of the internal state model.

In C lang, openssl offers a set of functions that allow for creating randomly generated numbers. Example usage:

```c
#include <openssl/rand.h>
#include <stdio.h>

int main() {
    unsigned char buffer[4];
    unsigned int random_number = 0;

    RAND_bytes(buffer, sizeof(buffer));

    for (int i = 0; i < 10; i++) {
        random_number = (random_number << 8) | buffer[i];
    }
    printf("Random number: %u\n", random_number);
    return 0;
}
```

Encoding and Decoding

Encoding and Decoding differ from Encryption and Decryption.

Encoding puts a data and labels it in a know format.
Decoding gets the data back from that known format.

Encryption is a type of encoding, but is a lot more complex, and uses a key to "encrypt" the data where the data would be encoded with added variability to secure it.
Decryption would decode that data using the access key.

Introduction to Cryptography

Allows for:

- Confidentiality
- Authentication
- Integrity
- Non-repudation

Keys:

- should be kept secret
- managed only on trusted systems
- should be of adequate length

Caesar Cipher

It works by shifting characters, the key would be the number of how many characters to shift by.
key=2
a -> c
b -> d
...
z -> b

Symmetric Cryptography

Use the same key for encryption and decryption.

Block Ciphers

Encrypt data in a fixed-sized blocks. (e.g. exactly 128 bits).

Stream Ciphers

Does bit-by-bit.

> Keys are Shared Directly

Block Ciphers

DES key of size 64 bits. 16 hex characters. Each 2 chars are 1 byte, each byte is 8 bits so 64 in total. (56 key with 8 parity)

ECB Electronic Code Block

Literally divided into blocks, each of proper size.
Those blocks can be differentiated and ordered, thus u might fall into known plain text attacks.

CBC Chaining blocks together.
Not parallel, order not shown.

Pick IV, xor it with p1 get c1, xor c1 with p2 get c2, xor c2 with p3...

To fill in shorter ones u can add block padding

Stream Ciphers

Encrypts the entire data block directly, does't divide into different blocks.

Basic Digital Signature

Is used for confidentiality, where the sender encrypts the data with the secret key, and the other side would decrypt it with the public key for that specific key, and thus identities are validated.

Provides confidentiality without a shared secret.

Asymmetric

Two keys are generated as a pair, one will be public the other private.

High Computational Load

- Not for data encryption.

RSA

Generation

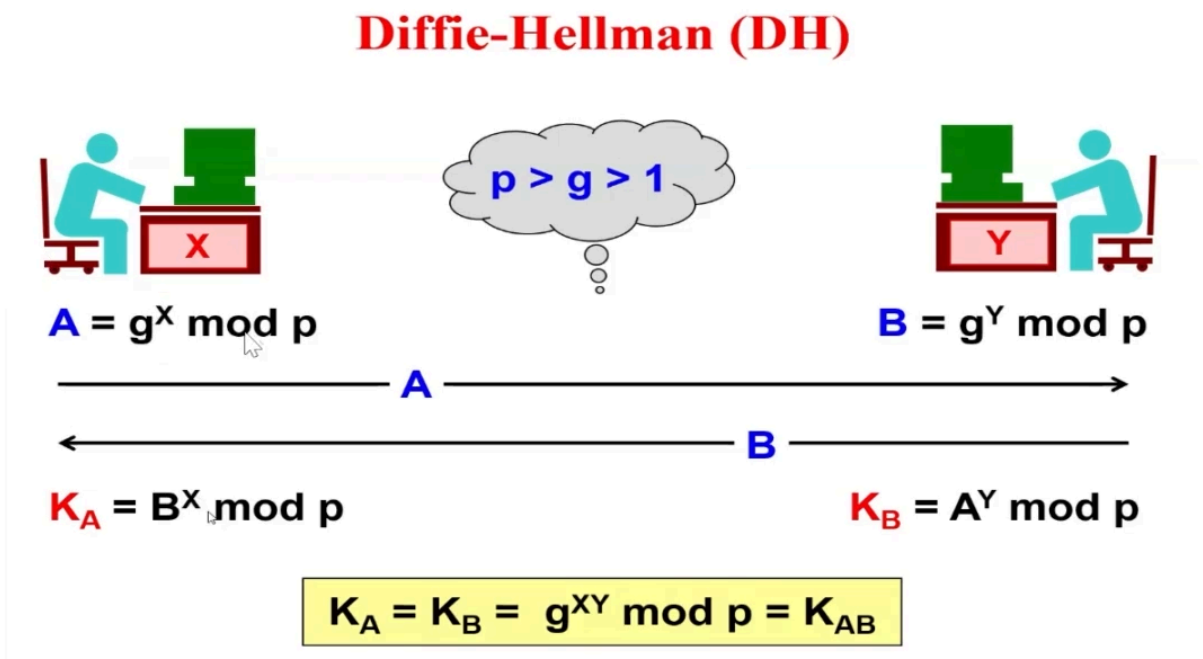
- Pick P & Q such that P & Q are secret large prime numbers.
- Public model N = P x Q
- PHI = (P - 1) (Q - 1)
- Public exponent E such that 1 < E < PHI, relatively prime to PHI (no common factors).
- Private exponent D = inv(E) mod PHI
- Public Key = (N, E)
- Private Key = (N, D)

Application

- Key size = Size of N
- RSA may cipher/decipher only data size < N
- Encrypt C = P^E mod N
- Decrypt P = C^D mod N
- (X^D)^E mod N = (X^E)^D mod N

Complexity depends on the number of bits with value 1 in E and D, most commonly used: 3, 17, 65537.

Diffie-Hellman



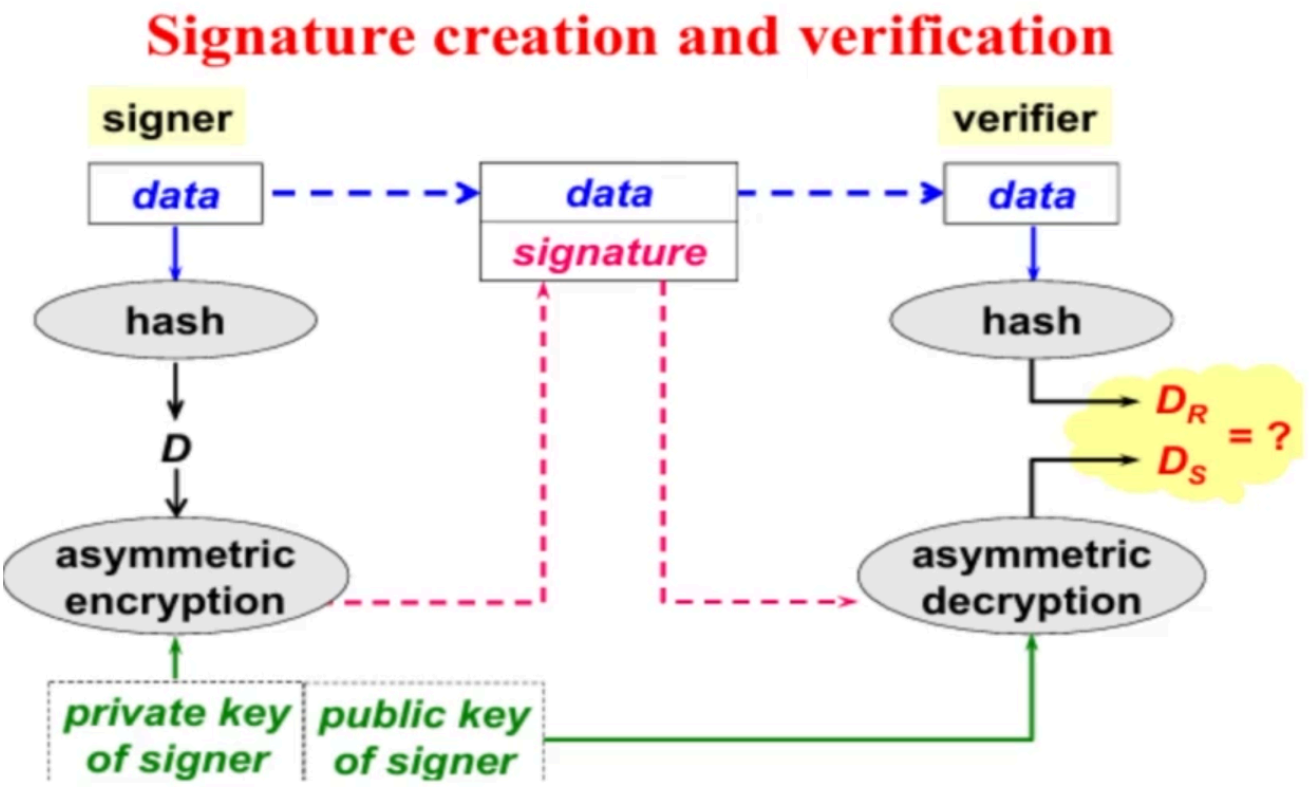
HASH

- Message Digest is fixed length summary of the message to be protected (of any length).
- Digest can be calculated in many ways, but usually via cryptographic hash function.
- The function must provide:
  - Fast computation
  - Pre-image resistance
  - Collision resistance

MAC MIC MID

- Message Authentication Code: add authentication
- Message Integrity Code: add a code
- Message Identifier: avoid replay attacks by adding specific code for each message.

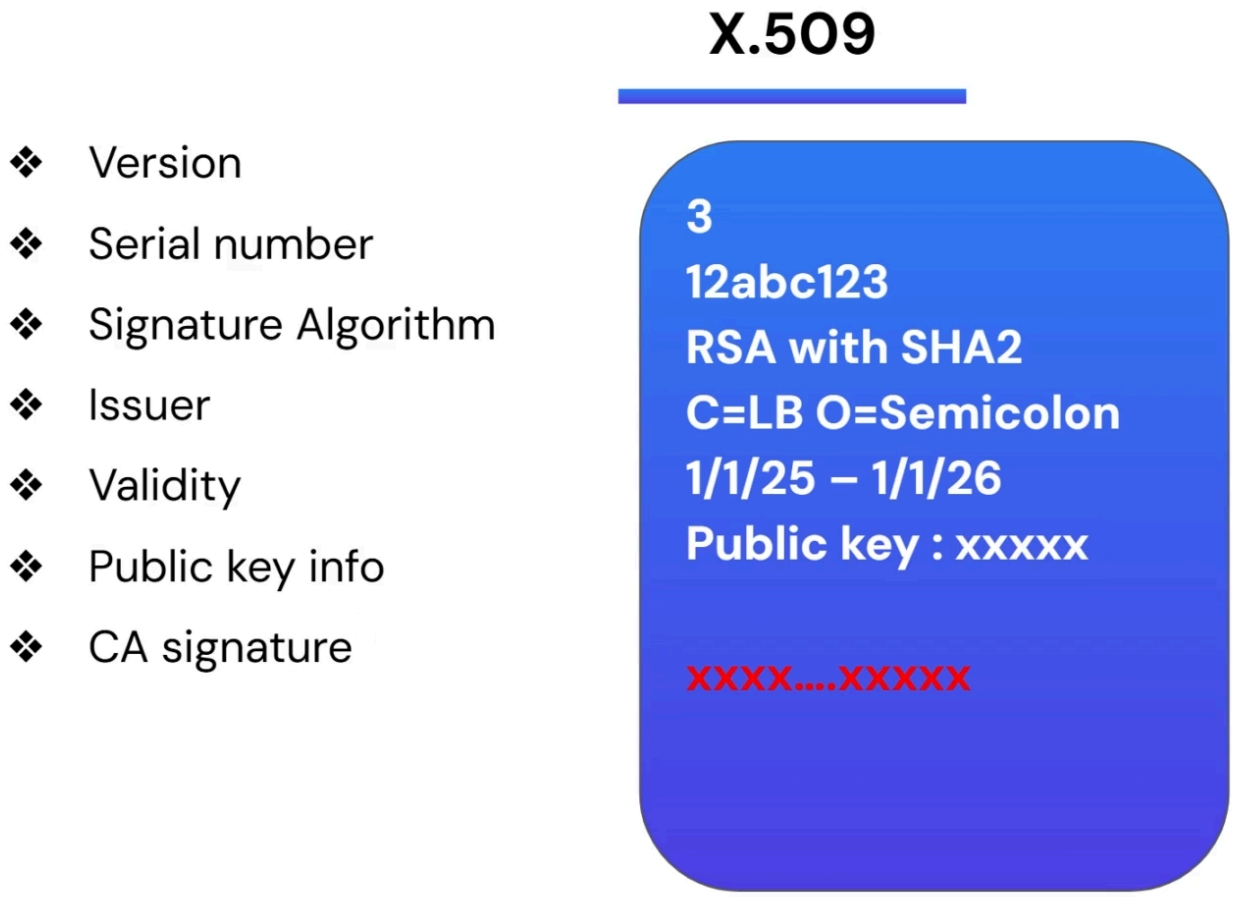
Digital Signature



Public Key Certificate

A structure used by a lot of services to securely bind a public key to some attributes.

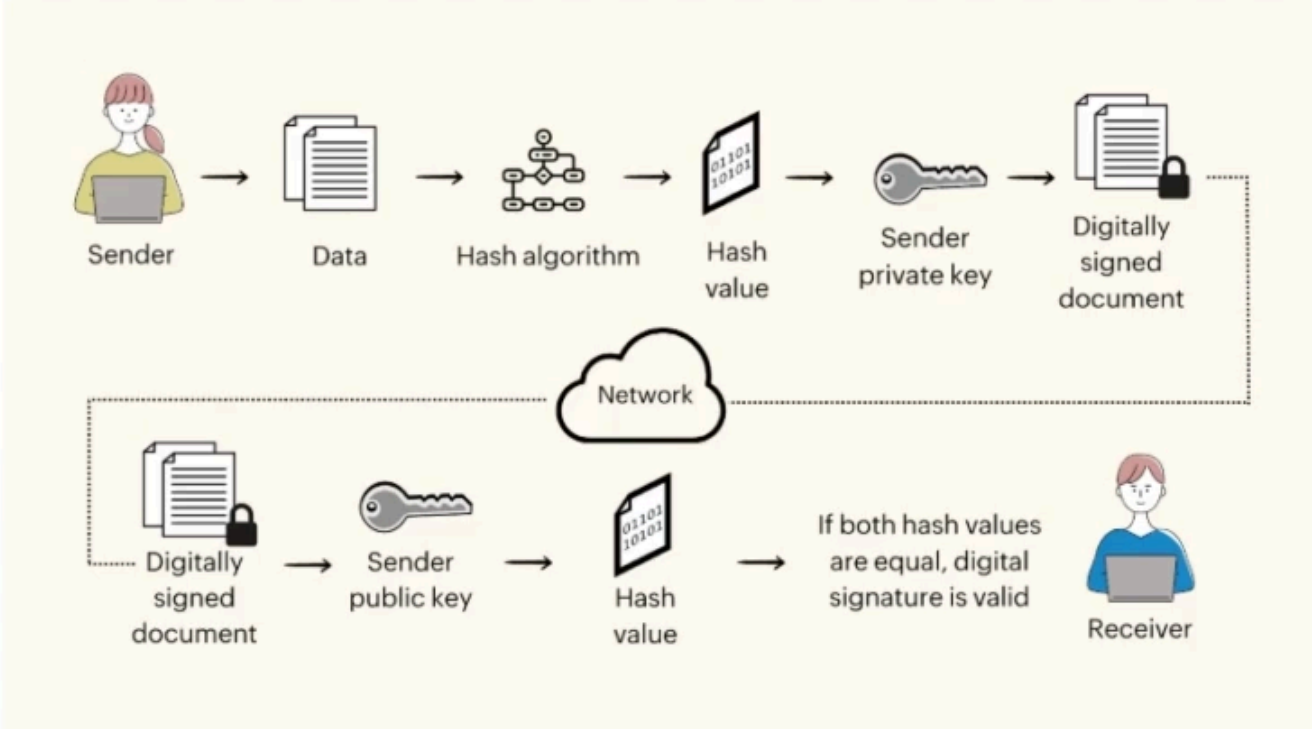
- Typically binds it to an identity or ip.
- Digitally signed by the certification authority (CA)
- Limited lifetime



Quick Recap

ON TLS

- syn-syn_ack-ack
- share public keys (diffiehellman)
- use encryption
- send data



Deauth Attack

Send death frames for the user.

Some Wireless Attacks

WEP hacking

WEP has encryption with a IV vector of only 24 bits, which means with enough packets (abt 5k packets) we can actually know what this IV is and replay it/xor it to get the data.

WAP/WPA2 hacking

Relies on a 4 way handshake

capture the handshake

brute force it.
