# Network security

## A close up of text on a white background Description automatically generatedWhat is network security?

**confidentiality**: only sender, intended receiver should “understand” message contents

sender encrypts message

receiver decrypts message

**authentication:** sender, receiver want to confirm identity of each other

**message integrity:** sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

**access and availability:**services must be accessible and available to users

In the following examples, Bob and Alice wants to communicate and Trudy(the intruder) wants to intercept, delete or add something to the message.

A picture containing game, drawing

Description automatically generated

Trudy has several options for what to do:

* Spoofing—The attacker uses someone else’s information to access the system.
* Tampering—The attacker modifies some data in nonauthorized ways.
* Repudiation—The attacker removes all trace of their attack, so that they cannot be held accountable for other damages done.
* Information disclosure—The attacker accesses data they should not be able to.
* Denial of service—The attacker prevents real users from accessing the systems.
* Elevation of privilege—The attacker increases their privileges on the system thereby getting access to things they are not authorized to do.

## Principles of cryptography

### When talking cryptography there are several topic specific words and phrases:

* M — Plain text message. Nothing is encrypted.
* KA (M) — Ciphertext, which is the plain text M encrypted with key KA.
* KB (KA (M)) — Decryption of the ciphertext with key KB. The output is then M.

### There are several ways to break the encryption scheme:

Cipher-text only attack: Trudy has ciphertext she can analyse. She can crack the encryption in two ways:

* brute force: search through all keys
* statistical analysis

Known-plaintext attack: Trudy has plaintext corresponding to ciphertext. Trudy knows both M and KA(M).

* chosen-plaintext attack: Trudy can get ciphertext for chosen plaintext

### Symmetric key cryptography

Bob and Alice share same key KS. The type of cryptography method used is knowing substitution pattern in mono alphabetic substitution cipher, DES, AES.

A picture containing clock, drawing

Description automatically generated

Mono alphabetic: <https://en.wikipedia.org/wiki/Substitution_cipher>   
DES: <https://en.wikipedia.org/wiki/Data_Encryption_Standard>   
AES: <https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

So how do Bob and Alice agree on a key?

A close up of a map

Description automatically generated

### Public key encryption

We need a key K+A and a key K-A.   
Then K-A (K+A(m)) = m.   
This means that the private key K-A can decrypt the ciphertext from the public key K+A.   
  
It should also never be possible to compute the private key out of the public key. Example is RSA encryption.

Also:

A picture containing bird

Description automatically generated

### RSA encryption in practice: Session keys

Alice and Bob establish a connection and uses RSA encryption to exchange a key for symmetric key encryption. This is because RSA encryption is very slow.

## Authentication

Authentication is very hard as Trudy can pose as a man in the middle.

A screenshot of a cell phone

Description automatically generated

## Message integrity

In the real world a person can sign a letter with their signature and the receiver can therefore verify the letters integrity.

### Digital signatures

Bob signs m by encrypt it with his private key K-B.

Then he sends both the signed message and the plain text message to Alice.

A screenshot of a cell phone

Description automatically generated

Alice verifies the message by applying Bobs public key to the encrypted message to see if it’s equal to the unencrypted message. If it is, then it must be sent by someone with Bobs private key (probably Bob).

As it is very expensive to compute private-key-encryption for large messages, a hash function is used to give the message a digital fingerprint.

The hash functions output has a fixed length H(m) which then is encrypted. It is almost impossible to reverse the hash function.

### Certification authorities

To fix the problem with a man in the middle, certification authorities (CA) are used to certificate messages. It binds a public key to an entity.

A screenshot of text

Description automatically generated

A screenshot of a cell phone screen with text

Description automatically generated

## Securing TCP connections: Secure Socket Layer (SSL)

A screenshot of a cell phone

Description automatically generated

Lets see how SSL works:

A cut in half

Description automatically generated

A close up of a map

Description automatically generated

### Key derivation

A screenshot of a cell phone

Description automatically generated

### Data records

A screenshot of a cell phone

Description automatically generated

A close up of text on a white background

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

## Network layer security: IPsec