Computer Science Basics
Symetric Cryptography

Fall Term 2026/2027

Dr. E. Benoist | BFH-TI

Cryptography

- **Symetric Cryptography**
  - Problem statement
  - Caesar Cypher
  - One time pad
  - Advanced Encryption Standard
  - Conclusion
- **Asymmetric cryptography**
  - Symmetric vs Asymmetric
  - Key Exchange: Diffie-Hellman
  - Conclusion
- **Public Key Infrastructure (PKI)**
  - Problem
  - Public Key Infrastructure
  - Certificate
  - TLS
- **Conclusion**

Symetric Cryptography

Problem

Alice and Bob want to communicate

- Their conversation must remain secret
- No one should be able to listen to the conversation
- Alice wants that only Bob can read the message
- Bob wants to be certain that the message comes from Alice

Protocol

- A and B define together a common key K
- A writes a message M
- A encrypts M with the key K
- the encrypted message MK' travels on the internet
- B reads MK' and uses K to decrypt

Results

- A is sure that only B can read her message (if the key remains secret).
- B is not sure if the message comes from A

Check Integrity

Addition to the protocol

- A must do a “checksum” of his message (cryptographic hash function) and put it in his message.
- If the decrypted message is consistent with the checksum, it comes from A
- (or someone who has stolen the key)

Caesar Cypher

Caesar's Cypher

- Used by Cesar for its secret messages

Substitution cipher

- A letter is replaced by a letter at a fixed distance
- For example: we decide that the distance (i.e. the key) is three letters to the right
- A becomes D,
- B becomes E,
- C becomes F,
- Bonjour becomes Erqmrxu

Decryption

- As the correspondent knows the key (shift 3 to the right) they can decypt the message
- Erqmrxu becomes Bonjour again

Existing protocols

Examples of protocols

- One time pad
- DES (Data Encryption Standard (or 3DES) considered too weak
- AES (Advanced Encryption Standard),
- Blowfish, $CAST_5$, RC_4, RC_5, RC6, and IDEA

What is symetric encryption used for

It is faster than asymetric encryption (see next week)

- Faster Encryption
- Used for bulk Encryption / Encrypting large amounts of data

Examples

- TLS uses symetric encryption to send data for web pages (https)
- All the algorithms used in real life use symetric algorithms for encryption of data.

One time pad

The only one algorithm to be proven secure

- Proof by Shannon in the 1940s (publication 1949)

Encryption

- The key K used to encrypt a message M has the same length than M
  length(K) = length(M)
- The key is used only once (need a new key with each new message)
- To encrypt the message one to an XOR
  M' = M XOR K

Decryption

- Two times XOR is returning to the original message
  M = M' XOR K

One time pad

Very secure

- bits in M' are totally random (if K is random)
- knowing M' and not K, ANY message can be obtained with a different key K'.
- Knowing M' and the message you think is good, you can always generate K'.

Must be used only once

- If used twice, the messages can be used to find the key.

AES - Advanced Encryption Standard

Successor of DES (Data Encryption Standard)

- DES was proven week, (key length 56bit)
- NIST (National Institute of Standards and Technology) organized a contest
- Algorithm Rijndael won

Block cypher

- Data is split in Blocks of 128 bits

Supports various key lengths

- 128, 192, 256 bit

AES

Advantages

- AES is very fast
- Can be software implemented
- Can be hardware implemented

Quite secure

- There is no known attacks for a correct implementation of AES

Conclusion on symetric cryptography

Problem

- Alice and Bob must share the same key
- Alice and Bob must know each other
- How to do it on the Internet?
- I don’t know Google or Facebook

Asymmetric cryptography

Asymmetric cryptography I

Alice wants to send a message to Bob

- But Alice doesn't share any secrets with Bob.
- Bob has a key pair (public key, private key)
- Suppose Alice had knowledge of Bob's public key

Alice encrypts the message

- Alice uses Bob's public key to encrypt the message
- She's sending the message to Bob.
- No one other than Bob can read the message

Bob receives the encrypted message

- He uses his private key to decrypt the message

Asymmetric cryptography II

Algorithms

- RSA (Rivest Shamir and Adelman 1978)
  Multiplication / Factoring
- ElGamal
  Exponentiation / Discrete logarithm

Problem

- Bob can't be sure the message is from Alice.
- Bob can't be sure the message hasn't been changed by someone else

Asymmetric key signature

Alice also has a key pair

- Alice has a pair (private key, public key) too
  Bob knows Alice's public key.

Alice can sign a message

- Alice uses her private key
- She signs her message with the private key
- She's the only one who could sign with this key and anyone can.
- check with the public key (cryptographic property of the asymmetric cryptographic key protocols)

Bob can check that the message is from Alice

- Bob uses Alice's public key to verify that the message comes from Alice

Problem: Key exchange

How to know the public key

- Alice or Bob can give themselves the public keys physically
- publish the keys on public servers
- send the keys by email
- Attach the keys to their messages
- **Problem:** how to know if it’s the right key

Trusted third party

- A certification authority (CA) will "validate" a certificate
- Alice and Bob must have confidence in this board
- Alice and Bob must know the public key of the CA

The Board will certify the relationship between an "identity" and a public key

- A certificate is signed by the board for Alice and Bob
- Contains Alice’s (resp. Bob) identity and public key, all signed by the Board of Directors.

Symmetric vs Asymmetric cryptography

Symmetric key cryptography is fast

- AES, has been designed to be very efficient

Asymmetric key cryptography is slow

- Can not be used to transfer large data

Protocol mix both types

- Use public key infrastructure to exchange public keys (PKI see next week)
- Generate a new session key (symmetric key).
- Encrypt large amount of data using the session key
- Encrypt the session key using the public key of the recipient.
- Send the encrypted message and the encrypted key.

Key Exchange: Diffie-Hellman

Public key protocol to exchange secret keys

- conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman (1978).

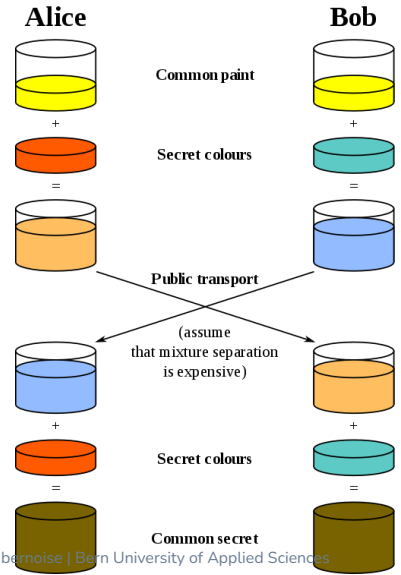
Alice and Bob want to generate a shared (symmetric) key

- They agree on one value (not secret)
- Each of them selects a private key
- Each send a message (value + private key)
- The final key is (value + private key A + private key B)

Mathematics to be used

- Multiplicative groups:
  For instance: integers modulo p (prime number)
  or elliptic curves.

Diffie-Hellman



Conclusion on asymetric cryptography (aka public key crypto)

Public key cryptography is very slow

- Symmetric cryptography is much faster

Used to communicate with unknown persons

- Just need the public key

Need to communicate securely public key

- Public Key Infrastructure (PKI) : Next Week

Public Key Infrastructure (PKI)

Problem: Key exchange

How to know the public key

- Alice or Bob can give themselves the public keys physically
- publish the keys on public servers
- send the keys by email
- Attach the keys to their messages
- **Problem:** how to know if it’s the right key

Trusted Third Party

- A certificate authority (CA) will "validate" a certificate
- Alice and Bob must have confidence in this board
- Alice and Bob must know the public key of the CA

The CA will certify the relationship between an "identity" and a public key

- A certificate is signed by the CA for Alice and Bob
- Contains Alice’s (resp. Bob) identity and public key, all signed by the CA.

PKI Architecture

Public Key Infrastructure (PKI)

- Allows a secure key exchange
- A prerequisite for the use of public key cryptography

Central role: the Certificate Authority (CA)

- Everyone knows their public key
- Uses their private key to sign new certificates

A certificate

- The identity of the holder.
- The holder's public key.
- The identity of the CA.
- The signature made by the CA.

Alice and Bob

- Can exchange their certificates;
- test the validity of these certificates (i.e. public keys);
- trust the other's certificate.

Certificate Information

X509 certificates

- Used by websites to ensure the "handshake" of TLS.
- TLS is used by https, sftp, …

At least

- Server name
- Public key
- identity of the Certificate Authority
- Protocols used for signature

Supplementary information

- Identity of the holder
- Physical address of the holder

Google.com certificate

```
Certificate Information:
Common Name: www.google.com
Subject Alternative Names: www.google.com, google.com
Organization: Google Ltd.
Organization Unit: Tech Dept.
Locality: English
State: Florida
Country: US
Valid From: March 14, 2011
Valid To: March 14, 2014
Issuer: UTN-USERFirst-Hardware, The USERTRUST Network Write review of Comodo
Key Size: 2048 bit
Serial Number: f5c86af36162f13a64f54f54f6dc9587c06
```

Content of a certificate?

Certificates are stored in coded form

- coded $\neq$ encrypted
- anyone can "decode

Open SSL

- Open Source Library for cryptography
- Possibility to create a whole PKI infrastructure (including a CA)
- Ability to read X509 certificates
- `openssl x509 -in certificate.crt -text -noout`

Website

- `http://www.sslshopper.com/certificate-decoder.html`

Transport Layer Security (TLS)

Internet protocols for secure connections

- Base for HTTPS, SFTP, ...

Goal: communicate securely with a server

- Be sure to communicate with the right server
- Make sure only the server can read what you send.
- I'm sure what we're receiving is coming from the server

Means

- A PKI architecture
- The server certificate

Problems

- Public key cryptography: very slow and consumer of computation time.
- secret key cryptography (symmetrical) : fast, but requires knowing each other.

TLS Handshake

Use public key cryptography (asymmetric)

- We download the certificate from the server
- We're checking this certificate
- We establish an encrypted communication with the server
- Together we define a secret key (new one that only serves once)

The protocol continues with this secret key

- Symmetric cryptography, much more efficient

Principle

- First of all, we don't know each other,
- We exchange business cards (and check them)
- Then we know each other and we can talk faster

Problems with TLS

TLS is often used as single security measure

- Often rely only on the certificate of the server
- Can be configured to use 2 certificates (1 for client, 1 for server).

List of Certificate Authorities

- Which ones are trusted?

How to update certificates for CAs

- Not an easy task,
- Very sensitive.

What if a certificate is corrupt?

Certificate can be corrupt if private key is stollen

- Stollen by an employee
- Hacked on the server
- Brute forced by an attacker
- Not considered secure anymore

Need to limit the validity of a certificate

- Certificates must contain a validity date

Revocation Lists

- Certificate authorities provide lists of revoked certificates : *Revocation Lists*.

Application should

- Have a list of valid CAs (the ones we trust)
- Should check for the revocation list
- Should not accept a certificate issued by a not trustworthy CA.

Conclusion

Conclusion

Cryptography

- Public Key cryptography (asymmetric)
- Secret Key cryptography (symmetric)

Protocols

- Mix both systems
- Asymmetric crypto to start (using Diffy-Hellman for instance).
- Then symetric crypto to send payload (data).

Public Key Infrastructure

- To transmit public key.
- To be certain the public key belongs to one person (or identifier).