Computer Science Basics
Asymmetric Cryptography

Fall Term 2023/2024

Emmanuel Benoist | BFH-TI

Asymmetric Cryptography

Last Week

Last Week

Symmetric cryptography

- 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
- **Eliptic Curves**
  Exponentiation / Discrete logarithm with much shorter keys
  Courves:
  - Curve25519 : For Diffie-Hellman key exchange
  - ED25519 : used for signing in ECDSA et EdDSA
  - secp256k1 : used in signatures for Bitcoin.

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

Symmetric vs Asymmetric

Symmetric vs Asymmetric cryptography

Symmetric key cryptography is fast

- AES, has been designed to be very efficient

Asymmetric key cryptography is slow

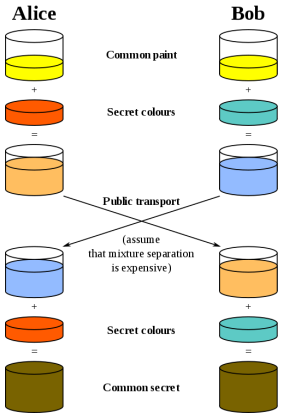
- Can not be used to transfer large data

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

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.

Conclusion

Conclusion

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