1 Crypto Recap

1.1 Objectives:

- **Confidentiality**
- **Integrity**
- **Authenticity**
- **Availability**
- Authorization
- Non-Repudiation, Accountability
- Freshness
- Anonymity, Unlinkability
- Intervenability, Contro
- Transparency

1.2 Confidentiality-Encryption

1.2.1 Symmetric Ciphers

- Secret key for en- and decryption
- Much more efficient
- **Block cipher:** encryps a plaintext block of fixed len e.g.: *Advanced Encryption Standard (AES)*
- **Stream cipher:** encrypts a bitstream e.g.:*ChaCha20*

1.2.2 Asymmetric Ciphers

- Public key for encryption
- Private key for decryption
- Ex.: RSA-based encryption

1.3 Integrity, Authenticity-Signatures, MACs

1.3.1 MACs

- Symmetric cryptography
- Protects data integrity & authenticity
- Ex.: Hash-based MAC

1.3.2 Digital Signatures

- Asymmetric cryptography
  - **Signing with** private key
- Protects data integrity & authenticity
- Provices non-repudation

1.4 Block Cipher Modes of Operation

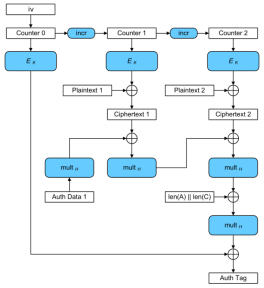
1.4.1 Electronic Code Book (ECB)

- Each plaintext block is encrypted seperatly
- Inherintly insecure! -> Smae block = Same cipher

1.4.2 Cipher Block Chainning (CBC)

- Plaintext is chained to previous ciphertext by XOR and encrypted afterwards
- Difficult to apply securely -> implementations often vulnerable

1.4.3 Galois Counter Mode (GCM)



2 Tranport Layer Security (TLS)

2.1 TLS handshake protocol

- Parameter Negotiation
- Key exchange
- Authentication

2.2 TLS record protocol

- Protection of integrity, authenticiy and confidentiality
- **Symmetric Cryptography:** e.g., block cipher, usually AES