Applied Cryptography

Arnab Roy

06 March, 2025

University of Innsbruck

Suggestions

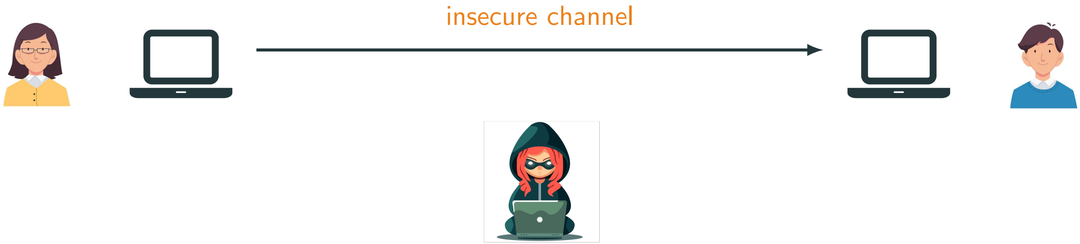
To perform well in this course

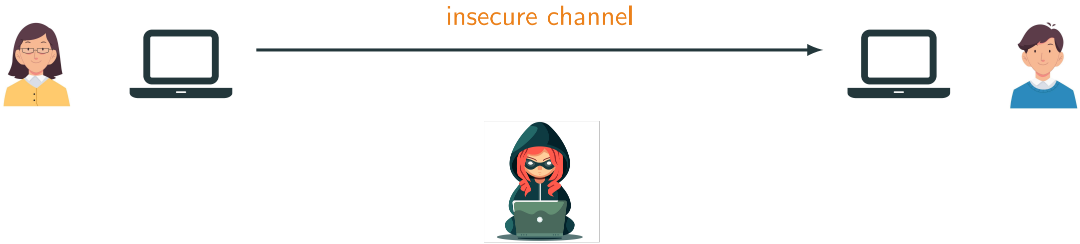
- Follow the topics from lectures: solve the given problems
- Ask (questions) if you can not solve them
- Go through the suggested reading: ask if you face difficulties
- Take notes during lecture
- I encourage discussing with your colleagues (on a topic or problems)

Recommended textbook: C. Paar, J. Pelzl: *Understanding Cryptography*

Introduction to Cryptography

Communication security

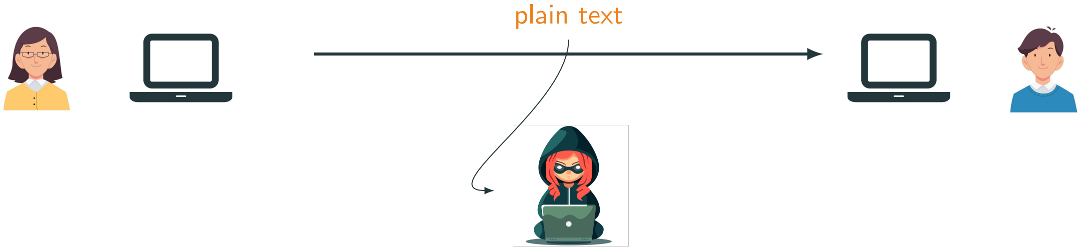




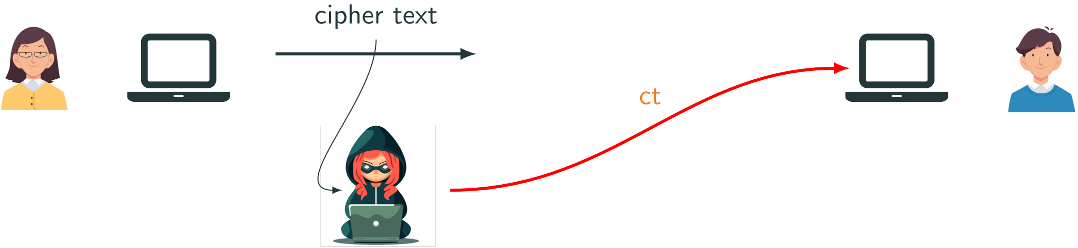
Security aims (data in communication or under storage)

- **Confidentiality**: Adversary must not be able to **read** message m
- **Integrity**: Adversary must not be able to **modify** message m
- **Authenticity**: Receiver should be able to ensure that m orginated from sender

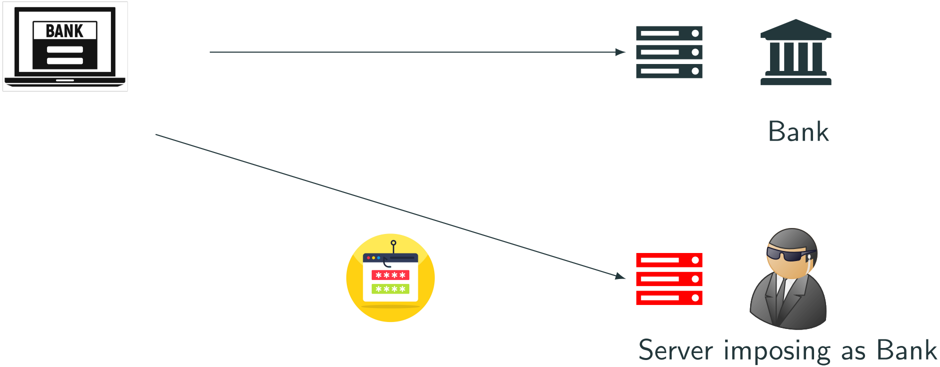
Confidentiality or secrecy



Integrity



Authentication



Adversary

Adversarial powers

Adversarial goals

Adversary

Adversarial powers

- With finite computing power: computational security
- Access to physical device and implementations (observable or subject to manipulation): side channel security or implementation security (not covered in this course)
- Unlimited computational power: information theoretic security or perfect secrecy (not covered in this course)
- Access to input and output: choosing or obtaining plaintext(s) and/or ciphertext(s)

Adversarial goals

Adversary

Adversarial powers

- With finite computing power: computational security
- Access to physical device and implementations (observable or subject to manipulation): side channel security or implementation security (not covered in this course)
- Unlimited computational power: information theoretic security or perfect secrecy (not covered in this course)
- Access to input and output: choosing or obtaining plaintext(s) and/or ciphertext(s)

Adversarial goals

- Recovering secret key: allows to read all messages encrypted with that key
- Plaintext recovery: recovering plaintext(s) from observable or choosen ciphertexts

General adversarial (attack) models

- Ciphertext only: adversary gains access to ciphertexts
- Known plaintext: access to $(x, \mathrm{Enc}(x))$ but no control over plaintext
- Chosen plaintext: chooses x and obtains corresponding $\mathrm{Enc}(x)$
- Chosen plaintext (adaptive): choose x_1 and obtains $\mathrm{Enc}(x_1)$; then chooses x_2 and obtains $\mathrm{Enc}(x_2)$
- Known ciphertext: access to $(y, \mathrm{Dec}(y))$ but no control over ciphertext
- Chosen ciphertext (adaptive)

Black box security and beyond

Security against generic attacks

- Adversary only have access to input and/or outputs from Enc
- No knowledge of Enc algorithm or its description

Opening the box: Adversary knows the algorithm or function description of Enc (cryptanalysis)

Side-channel: Adversary knows the algorithm and additional information from the execution of the algorithm [NOT covered in this course]

Symmetric Cryptography

Syntax of symmetric encryption

Symmetric encryption $\mathcal{E} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$

- $\mathsf{Gen}(\kappa) \xrightarrow{\$} sk$
- $\mathsf{Enc} : \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$ s.t $\mathsf{Enc}(x, sk) = y \in \mathcal{C}$
- $\mathsf{Dec} : \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ s.t $\mathsf{Dec}(y, sk) = x \in \mathcal{M}$
- $\mathsf{Dec}(\mathsf{Enc}(x, sk), sk) = x$ (correctness)

Note: Given a fixed $k \in \mathcal{K}$, the $\mathsf{Enc}(\cdot, k)$ is a permutation $(|\mathcal{M}| = |\mathcal{C}|)$

- **Qn**: Let $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ how many different permutations $f : \mathcal{M} \rightarrow \mathcal{C}$ are there?
- **Qn**: If $\mathcal{K} = \{0,1\}^m$ how many permutations are possible to have with Enc?

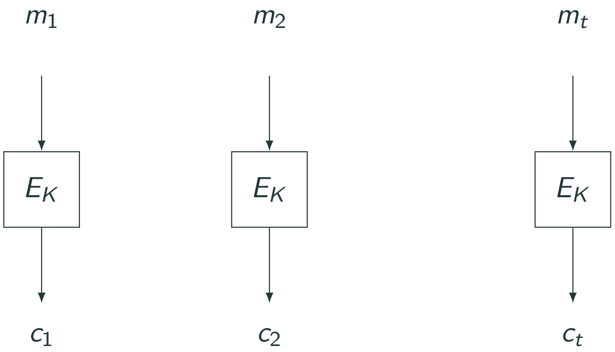
Block Ciphers and Modes of Operation

- Block ciphers are fixed length primitives
    - AES (Advanced Encryption Standard) can process 128 bits of input, key size = 128, 192 and 256 bits
    - DES (Data Encryptioin Standard): input size = 64 bits, key size = 56 bits

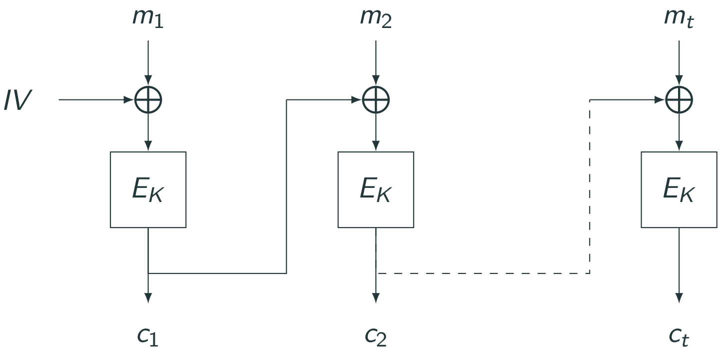
❓ How to encrypt data with arbitrary length? Secure mode of operation

- Examples: ECB, OFB, CBC, CTR, GCM

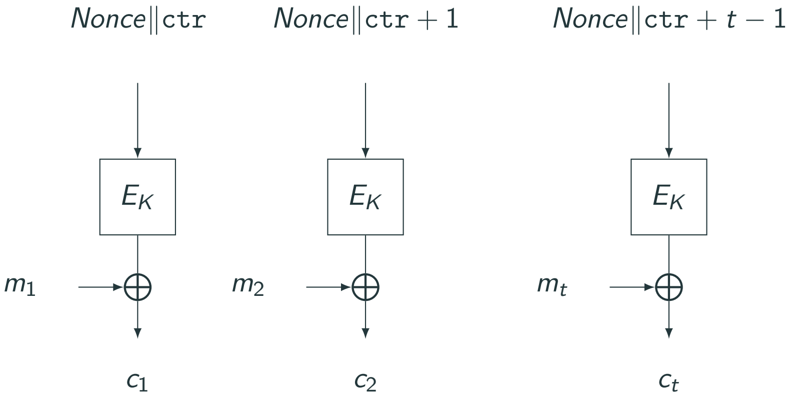
Electronic Code Book (ECB) Mode



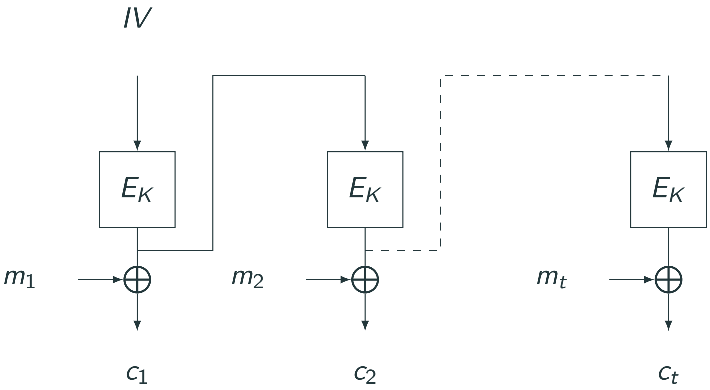
Cipher Block Chaining (CBC) Mode



Counter (CTR) Mode



Output Feedback (OFB) Mode



Applications

Symmetric-key crypto (SKC) is everywhere

- TLS: on our Web-browsers
- Cards: Payment cards
- Wireless communications: Wifi , Bluetooth
- Mobile communications:
- Encrypted data storage:
- Crypto-currencies:
- ......

Thank you!