LDACS1310: Introduction to Applied Cryptography

Lecture 1: introduction and course outline

T. Peters, ***F.-X. Standaert***

UCLouvain Crypto Group, fstandae@uclouvain.be

Reminder



- Best way to enjoy lectures is to close laptops, take handwritten notes (on printed slides) and participate actively to discussions

Information security vs. cryptography

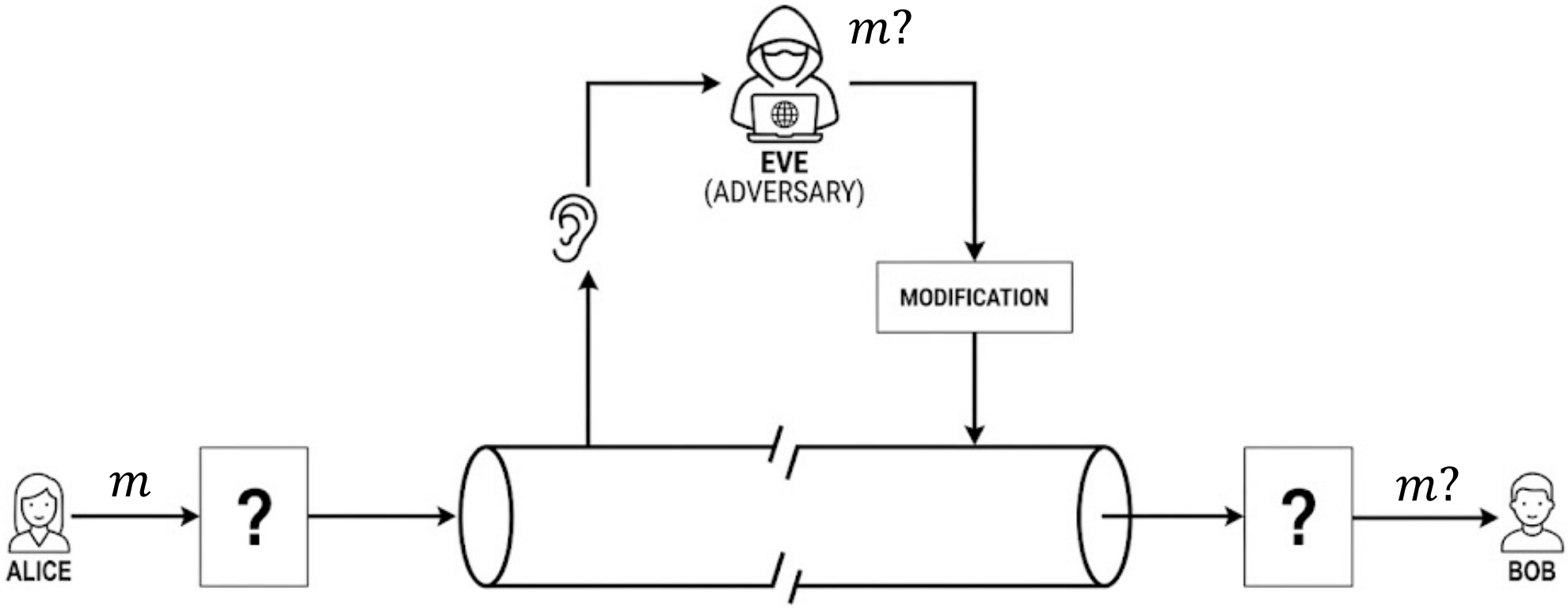
- Information security ≈ protecting digital assets from threats
  - Digital assets ≈ anything that has value:    …
  - Protecting ≈ ensuring security properties
    - Examples: confidentiality, integrity, availability, anonymity, …
  - Threats ≈ potential attacks against security properties
    - Examples: hardware (side-channels), software (buffer overflow), malicious hardware/software (Trojans, viruses), networks (sniffing), human (phishing), application-based (email/spam, AI), …

Information security vs. cryptography

- Information security ≈ protecting digital assets from threats
  - Digital assets ≈ anything that has value:    …
  - Protecting ≈ ensuring security properties
    - Examples: confidentiality, integrity, availability, anonymity, …
  - Threats ≈ potential attacks against security properties
    - Examples: hardware (side-channels), software (buffer overflow), malicious hardware/software (Trojans, viruses), networks (sniffing), human (phishing), application-based (email/spam, AI), …
- Cryptography ≈ mathematical background of information security

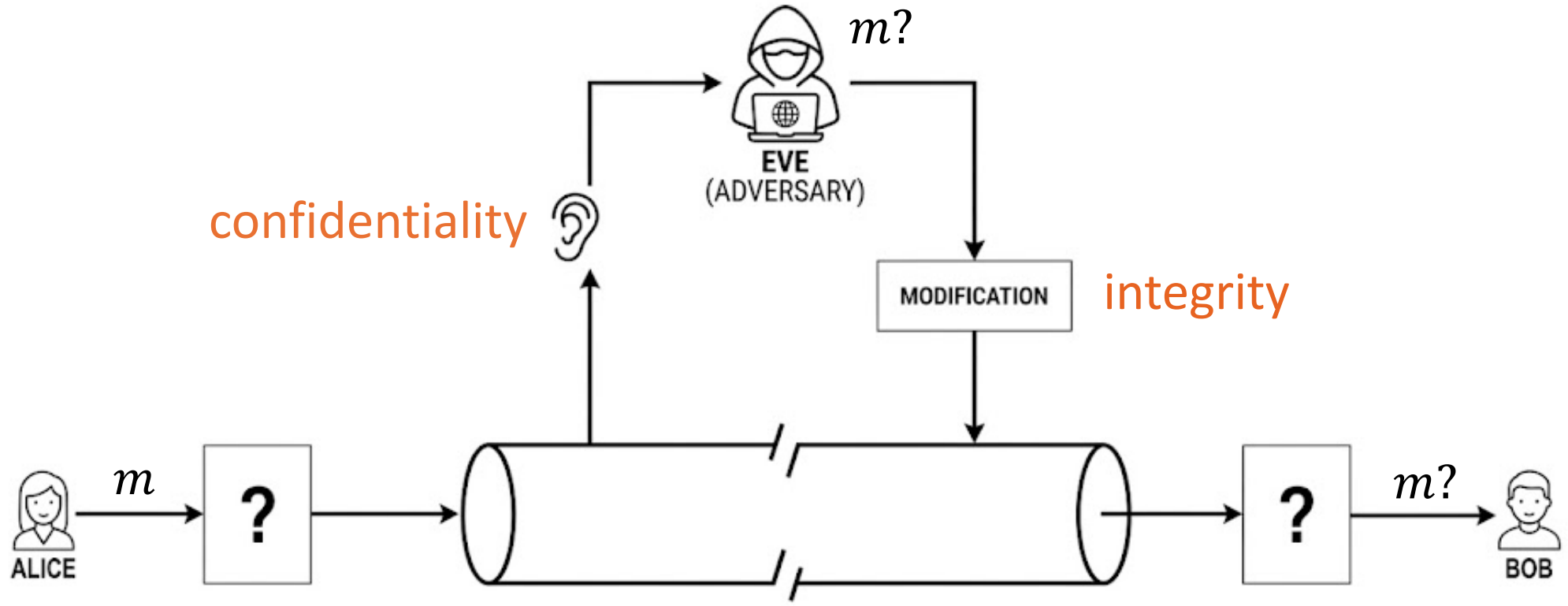
Example: secure communication

- Basic threat model: eavesdropping and man-in-the-middle



Example: secure communication

- Basic threat model: eavesdropping and man-in-the-middle



⇒ What to put in the rectangle boxes to prevent these threats?

Message confidentiality (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Symmetric encryption
Key generation: $k \leftarrow \mathrm{Gen}(n)$
Encryption: $c \leftarrow \mathrm{Enc}_k(m)$
Decryption: $m \leftarrow \mathrm{Dec}_k(\mathrm{c})$

Message confidentiality (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Symmetric encryption
Key generation: $k \leftarrow \mathrm{Gen}(n)$
Encryption: $c \leftarrow \mathrm{Enc}_k(m)$
Decryption: $m \leftarrow \mathrm{Dec}_k(\mathrm{c})$

Asymmetric encryption
Key generation: $(pk, sk) \leftarrow \mathrm{Gen}(n)$
Encryption: $c \leftarrow \mathrm{Enc}_{pk}(m)$
Decryption: $m \leftarrow \mathrm{Dec}_{sk}(\mathrm{c})$

- Case #2: similar but Alice & Bob do not share any secret

Message confidentiality (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Symmetric encryption
Key generation: $k \leftarrow \mathrm{Gen}(n)$
Encryption: $c \leftarrow \mathrm{Enc}_k(m)$
Decryption: $m \leftarrow \mathrm{Dec}_k(\mathrm{c})$

Asymmetric encryption
Key generation: $(pk, sk) \leftarrow \mathrm{Gen}(n)$
Encryption: $c \leftarrow \mathrm{Enc}_{pk}(m)$
Decryption: $m \leftarrow \mathrm{Dec}_{sk}(\mathrm{c})$

- Case #2: similar but Alice & Bob do not share any secret

⇒ Which properties are required for secure encryption?

Message integrity (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Msg. Auth. Code (MAC)
Key generation: $k \leftarrow \mathrm{Gen}(n)$ Tag generation: $t \leftarrow \mathrm{Mac}_k(m)$ Tag verif.: $\mathrm{Ver}_k(m, t) = \top$ or $\perp$

Message integrity (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Msg. Auth. Code (MAC)
Key generation: $k \leftarrow \text{Gen}(n)$
Tag generation: $t \leftarrow \text{Mac}_k(m)$
Tag verif.: $\text{Ver}_k(m, t) = \top$ or $\bot$

Digital signature
Key generation: $(pk, sk) \leftarrow \text{Gen}(n)$
Signature: $s \leftarrow \text{Sign}_{sk}(m)$
Verif.: $m \leftarrow \text{Verif}_{pk}(m, s) = \top$ or $\bot$

- Case #2: similar but Alice & Bob do not share any secret

Message integrity (terminology & semantics)

- Case #1: Alice & Bob share a n-bit secret key k

Msg. Auth. Code (MAC)
Key generation: $k \leftarrow \text{Gen}(n)$
Tag generation: $t \leftarrow \text{Mac}_k(m)$
Tag verif.: $\text{Ver}_k(m, t) = \top$ or $\bot$

Digital signature
Key generation: $(pk, sk) \leftarrow \text{Gen}(n)$
Signature: $s \leftarrow \text{Sign}_{sk}(m)$
Verif.: $m \leftarrow \text{Verif}_{pk}(m, s) = \top$ or $\bot$

- Case #2: similar but Alice & Bob do not share any secret

⇒ Which properties are required for secure MACs & signatures?

Statistical security (Shannon, 1949)

- Say $m \in \{0,1\}^n$ and assume a uniformly distributed $k \in \{0,1\}^n$
- $c = \mathrm{Enc}_k(m) = m \oplus k$, $m = \mathrm{Dec}_k(c) = c \oplus k$
- Assume a ciphertext-only eavesdropping adversary

❑ Question: $\Pr(M|C = c) =$

Statistical security (Shannon, 1949)

- Say $m \in \{0,1\}^n$ and assume a uniformly distributed $k \in \{0,1\}^n$
- $c = \mathrm{Enc}_k(m) = m \oplus k$, $m = \mathrm{Dec}_k(c) = c \oplus k$
- Assume a ciphertext-only eavesdropping adversary

❑ Question: $\Pr(M|C = c) = \Pr(M)$

- Statistical security: not enough information to decrypt

❑ Question: is it enough if each bit of k is uniformly distributed? {…}
❑ Question: what if $c_1 = \mathrm{Enc}_k(m_1)$ and $c_2 = \mathrm{Enc}_k(m_2)$ {…}

Statistical security (Shannon, 1949)

- Say $m \in \{0,1\}^n$ and assume a uniformly distributed $k \in \{0,1\}^n$
- $c = \mathrm{Enc}_k(m) = m \oplus k$, $m = \mathrm{Dec}_k(c) = c \oplus k$
- Assume a ciphertext-only eavesdropping adversary

❑ Question: $\Pr(M|C = c) = \Pr(M)$

- Statistical security: not enough information to decrypt

❑ Question: is it enough if each bit of k is uniformly distributed? {…}
❑ Question: what if $c_1 = \mathrm{Enc}_k(m_1)$ and $c_2 = \mathrm{Enc}_k(m_2)$ {…}

- One-time pad unpractical: k can be used once and is as long as m

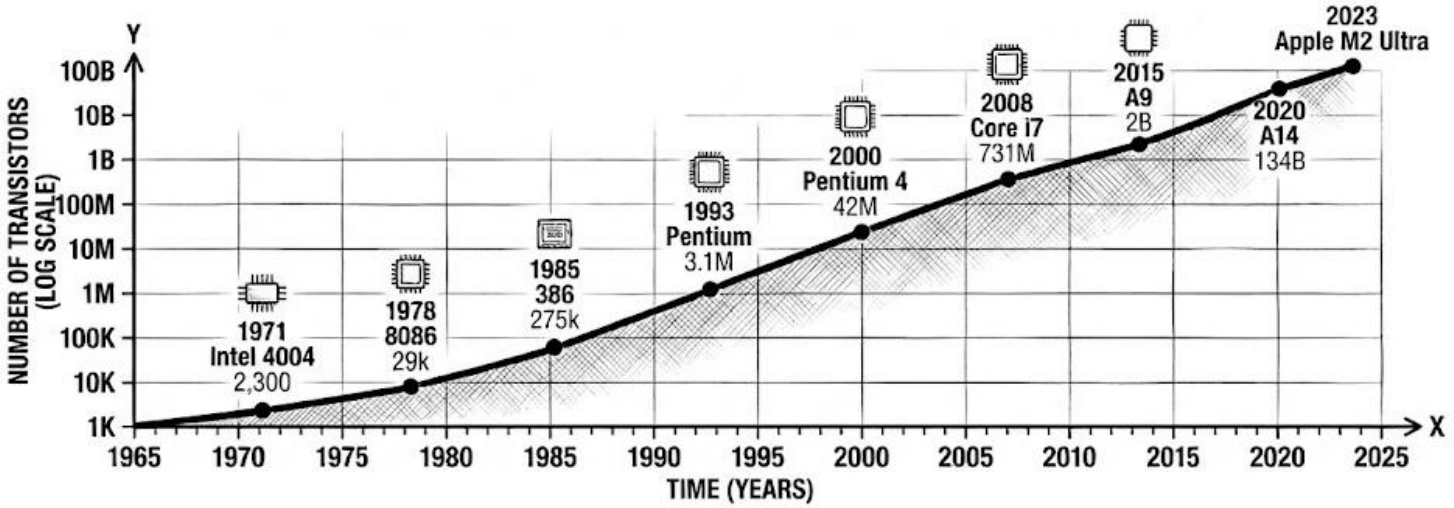
Computational security

- Say $m \in \{0,1\}^{n_m}$ and $k \in \{0,1\}^{128}$, $n_m \gg 128$, $c = \mathrm{Enc}_k(m)$
- Assume exhaustive key search is the only Adv strategy
  - Adv can test 2^{30} keys/sec with 1 computer
  - Adv can use $10^6 \approx 2^{20}$ computers

❑ Question: what is Adv's success probability in one year? {…}

Computational security

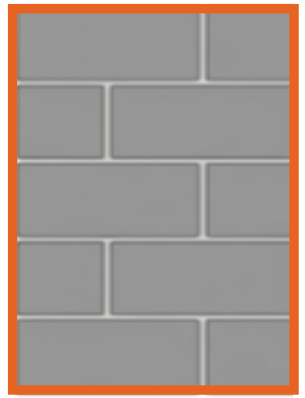
- Say $m \in \{0,1\}^{n_m}$ and $k \in \{0,1\}^{128}$, $n_m \gg 128$, $c = \mathrm{Enc}_k(m)$
- Assume exhaustive key search is the only Adv strategy
  - Adv can test 2^{30} keys/sec with 1 computer
  - Adv can use $10^6 \approx 2^{20}$ computers
- More practical but Adv's success probability evolves over time



- Question: more annoying for encryption or MAC and signatures? {…}

Cryptographic methodology

1. Define (the security properties that a scheme must satisfy)
2. Design (efficient schemes that hopefully satisfy these properties)
3. Argue about the security of the scheme in two steps
   a. Simplify: show that the security of complex schemes reduces to assumptions that are easier to analyze (e.g., that a lower-level problem is hard to solve)
   b. Cryptanalyze the simple(r) assumptions (≈ blocks)



Cryptographic methodology

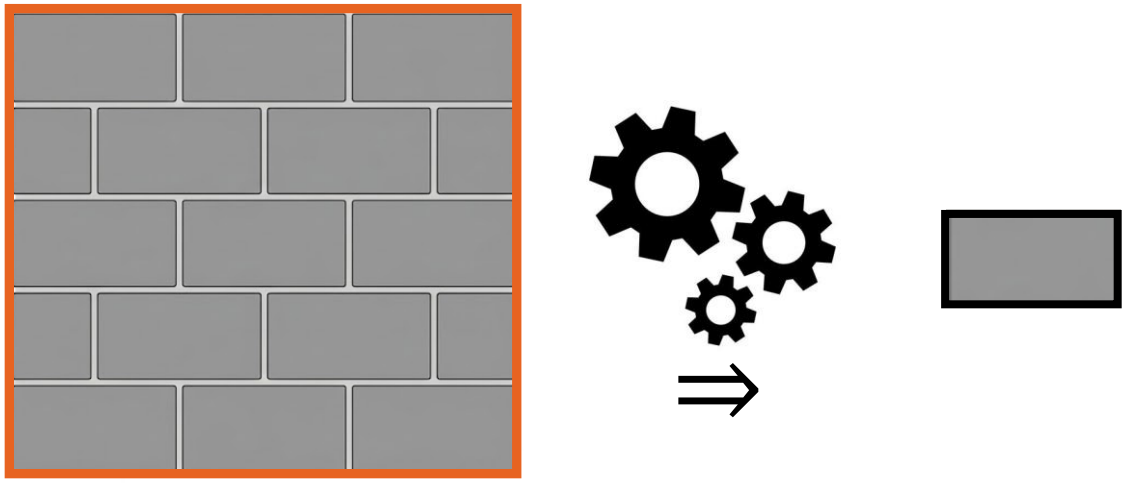
1. Define (the security properties that a scheme must satisfy)
2. Design (efficient schemes that hopefully satisfy these properties)
3. Argue about the security of the scheme in two steps
   a. Simplify: show that the security of complex schemes reduces to assumptions that are easier to analyze (e.g., that a lower-level problem is hard to solve)
   b. Cryptanalyze the simple(r) assumptions (≈ blocks)

4. Assuming everything is public information but the key



Security reductions

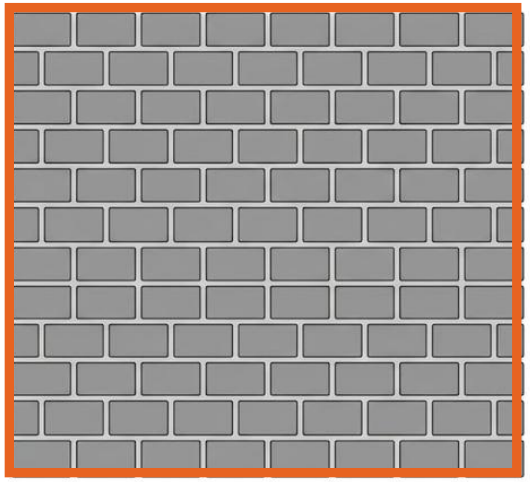
- The security of a cryptographic scheme S reduces to the hardness of a problem P if the hardness of P implies the security of S

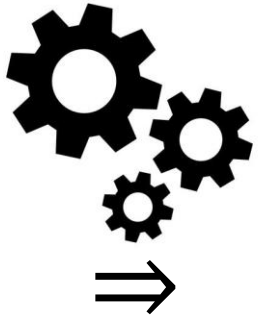


Contrapositive: an attack against the scheme S implies an efficient solution to the problem P

Security reductions

- The security of a cryptographic scheme S reduces to the hardness of a problem P if the hardness of P implies the security of S





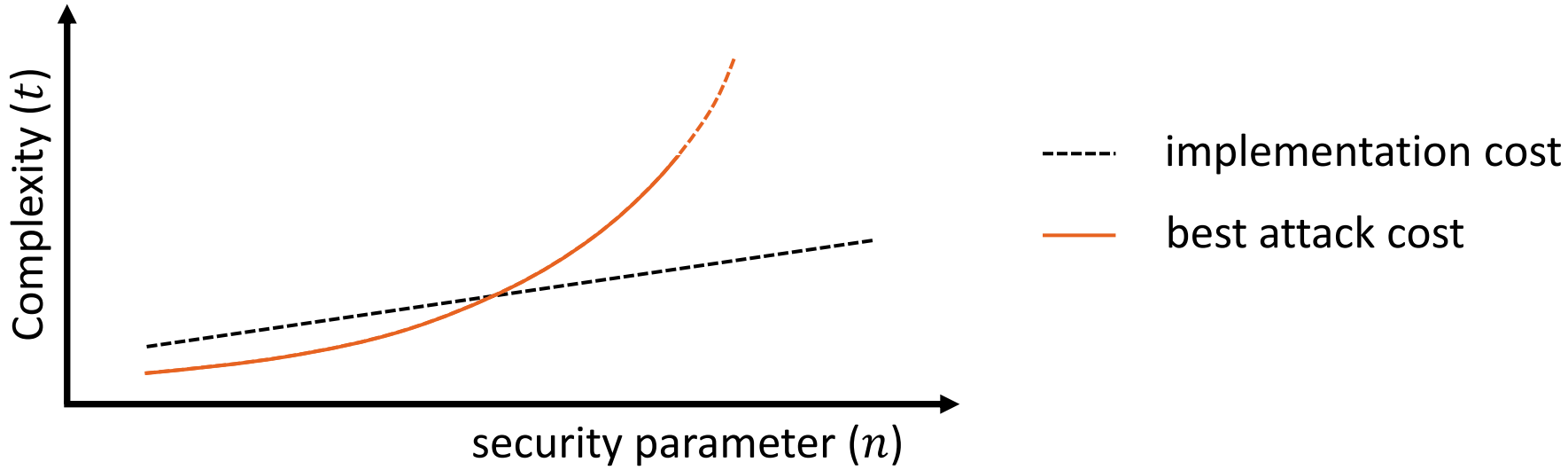


Contrapositive: an attack against the scheme S implies an efficient solution to the problem P

- Granularity dilemma: simpler assumptions give more confidence in the security but generally lead to less efficient schemes

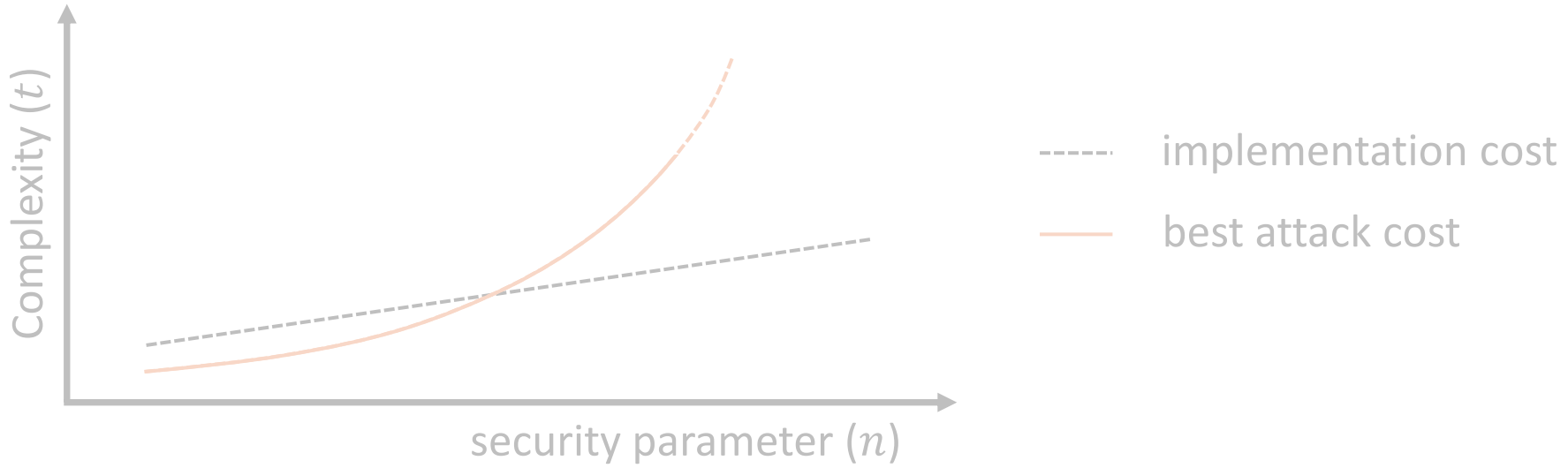
Concrete security

- General idea: create a gap between genuine users and Adv



Concrete security

- General idea: create a gap between genuine users and Adv



- Concrete approach: a scheme is (t, ε)-secure if any Adv running for time at most t breaks the scheme with probability at most ε

Asymptotic security

- Polynomial time Adv: runs in time $a \cdot n^b$ for constant a, b
- A scheme cryptographic S is secure if any polytime Adv succeeds in breaking S with only negligible probability $\mathrm{negl}(n)$
- A function f is $\mathrm{negl}(n)$ if, for every polynomial $\mathrm{p}(.)$, there exists a value N such that for all integer $i > N$, it holds that $\mathrm{f}(n) < \frac{1}{\mathrm{p}(i)}$

❑ Question: are 2^{-n} and n^{-1000} negligible functions {…}

Asymptotic security

- Polynomial time Adv: runs in time $a \cdot n^b$ for constant a, b
- A scheme cryptographic S is secure if any polytime Adv succeeds in breaking S with only negligible probability $\mathrm{negl}(n)$
- A function f is $\mathrm{negl}(n)$ if, for every polynomial $\mathrm{p}(.)$, there exists a value N such that for all integer $i > N$, it holds that $\mathrm{f}(n) < \frac{1}{\mathrm{p}(i)}$

❑ Question: are 2^{-n} and n^{-1000} negligible functions {…}

⇒ The security parameter can be used to reach any security level

Course approach

- Optimized cryptographic schemes can be hard to explain

⇒ Practicality explainability tradeoff: we look for a balance between

(a) Schemes that support the introduction/illustration of important concepts



Standard schemes that are recommended for practical use

Course approach

- Optimized cryptographic schemes can be hard to explain

⇒ Practicality explainability tradeoff: we look for a balance between

(a) Schemes that support the introduction/illustration of important concepts



Standard schemes that are recommended for practical use

- Lectures will usually start with (a) and end with a discussion of (b)
  (When possible, we use schemes that are practical and explainable)

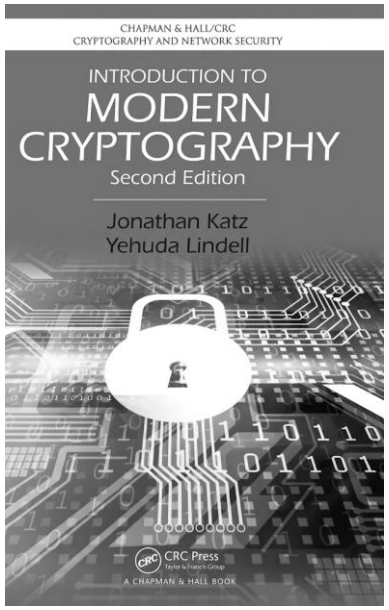
Course outline

- Topic 1: symmetric encryption
- Topic 2: block ciphers
- Topic 3: symmetric authentication
- Topic 4: asymmetric encryption
- Topic 5: digital signatures
- Topic 6: authenticated encryption
- Topic 7: post-quantum cryptography
- Topic 8: secure communication (TLS)
- Panorama of advanced topics

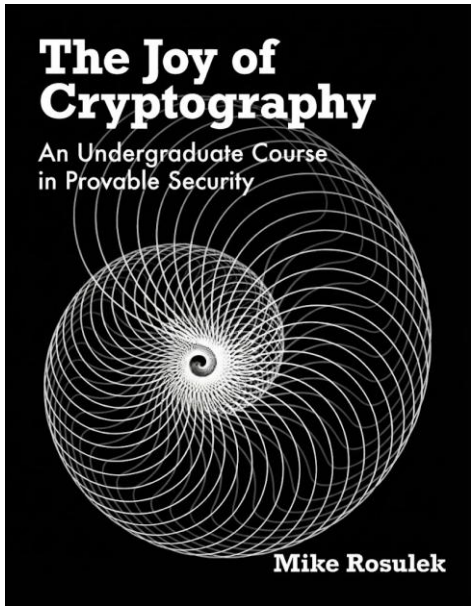
Course organization

- Lectures: Wednesday, 10:45 – 12:45
- Exercise sessions: Wednesday: 14:00 – 16:00
- Lecturers: Thomas Peters (thomas.peters@uclouvain.be) and François-Xavier Standaert (fstandae@uclouvain.be)
- Teaching assistants: Emilie Deprez (emilie.deprez@uclouvain.be) and Célia Lowagie (celia.lowagie@uclouvain.be)
- Course webpages:
  - https://perso.uclouvain.be/fstandae/LDACS1310
- Closed-book written examination

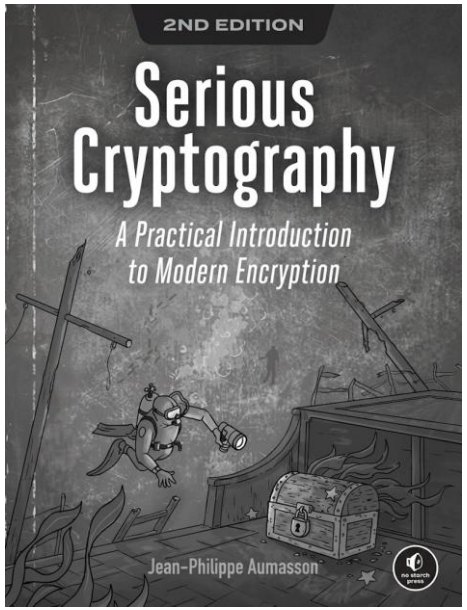
References



(a)



(b)



(c)

This lecture mostly follows the first three chapters of Reference (a). A general discussion of the goals of modern cryptography with an introduction to the one-time pad can be found in Chapters 1 & 2. The computational security setting, the concepts of concrete vs. asymptotic security and an introduction to reduction proofs can be found in Chapter 3. Reference (b) provides an alternative view to these topics. It also discusses the one-time pad and its limitations, an intuitive introduction to concept of provable security and the (asymptotic vs. concrete) computational security setting. Reference (c) discusses these topics in a less technical manner with a stronger focus on applications.

Questions?