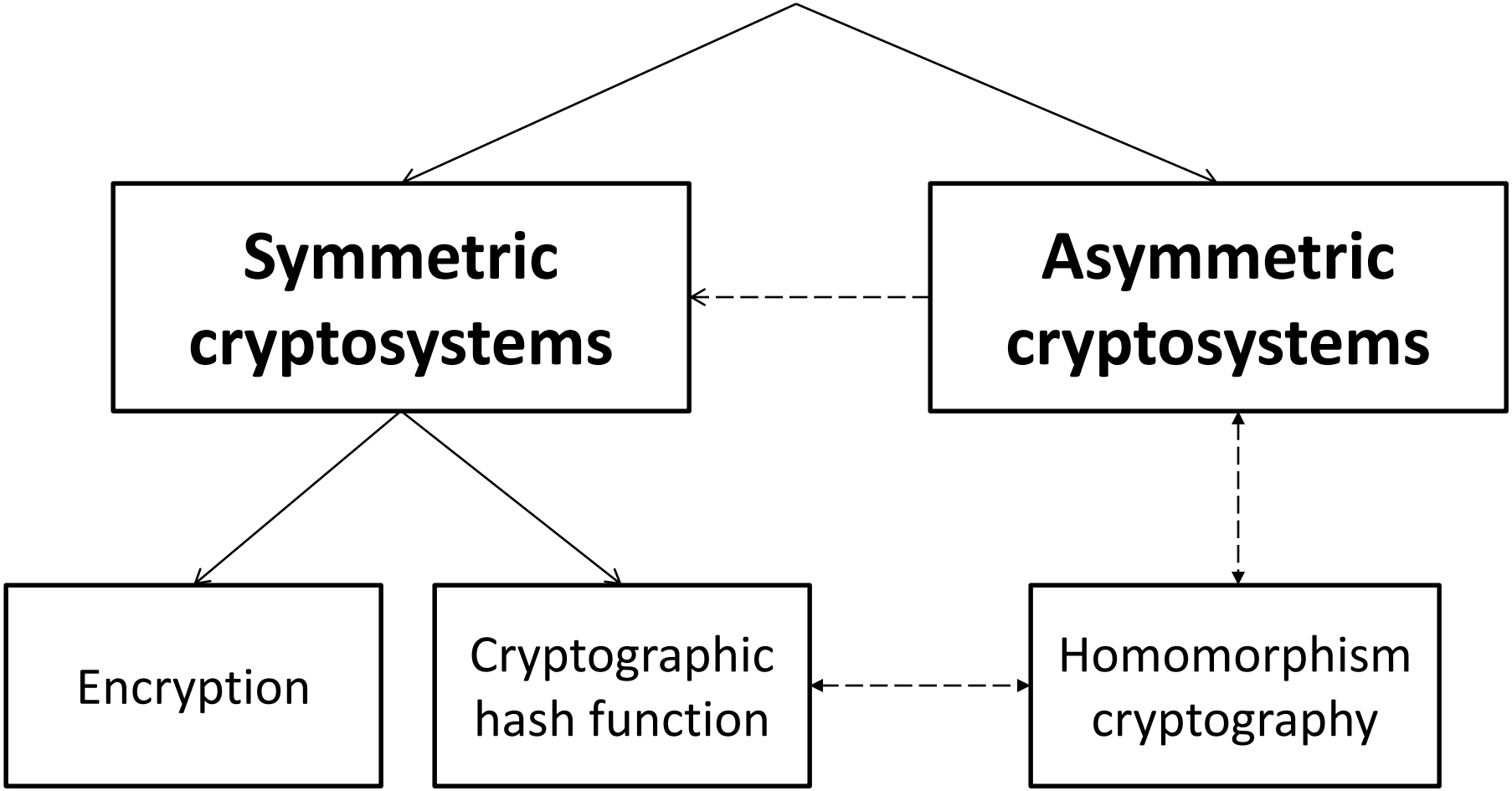
Applied Cryptography

Lecture 2

Cryptosystems



Definition

E_k: $\mathcal{M} \rightarrow$ C "Invertible"

$\exists E_{k'}^{-1} \equiv D_{k'}$: C$\rightarrow \mathcal{M}$ such that

$\forall m \in \mathcal{M}, k, k' \in K, c = E_k(m) \leftrightarrow m = D_{k'}(c)$.

Types of cryptosystem

- k $\neq$ k': Asymmetric cryptosystem/Public key cryptosystem.
- k $\equiv$ k': Symmetric cryptosystem/Secrete key cryptosystem.

- $|\mathcal{M}| \geq |$C$|$: cryptographic hash function.

Kerckhoff’s Principle

- The cryptosystem should be unbreakable practically, if not mathematically.
- Falling of the cryptosystem in the hands of an intruder should not lead to any compromise of the system, preventing any inconvenience to the user.
- The key should be easily communicable, memorable, and changeable.
- The ciphertext should be transmissible by telegraph, an unsecure channel.
- The encryption apparatus and documents should be portable and operable by a single person.
- Finally, it is necessary that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Attacks

- Attacks are typically categorized based on the action performed by the attacker. An attack, thus, can be **passive** or **active**
- Passive Attacks. The main goal of a passive attack is to obtain **unauthorized access to the information**.
- Active Attacks. An active attack involves changing the information in some way by conducting some process on the information.

Homomorphic cryptography

- In algebra, a **homomorphism** is a structure-preserving map between two algebraic structures of the same type (such as two groups, two rings, or two vector spaces).
- Some homomorphic cryptosystem
  - RSA
  - ElGamal
  - Paillier