Cryptography (and Information Security)
6CCS3CIS / 7CCSMCIS

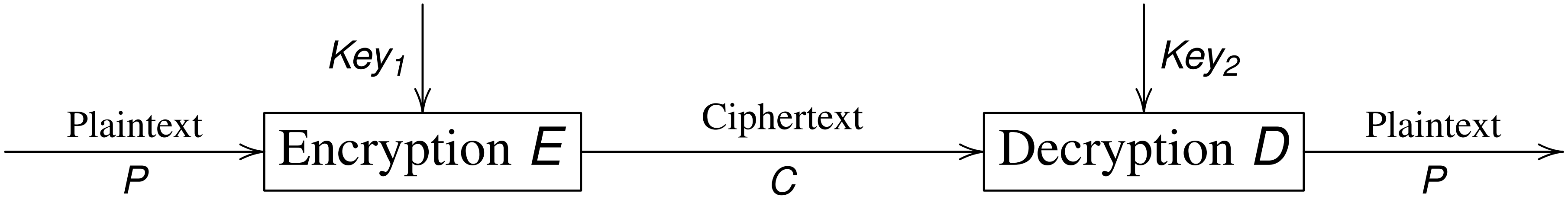
Prof. Luca Viganò

Department of Informatics
King's College London, UK

First term 2020/21

Lecture 2.2: A mathematical formalization of encryption/decryption

General cryptographic schema



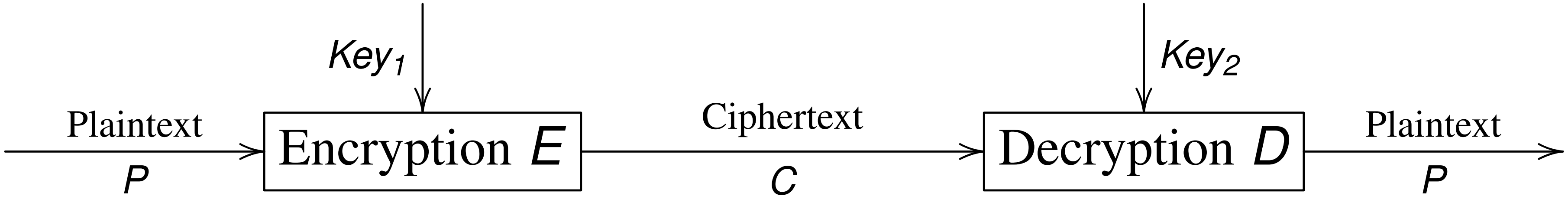
where $E(Key_1, P) = C$ and $D(Key_2, C) = P$.

Terminology

- **Plaintext** (or **plain text**, **clear text**, ...): text that can be read and "understood" (e.g., by a human being).
- **Encryption**: transformation (or function, process, procedure, ...) E that takes in input a plaintext and a key and generates a ciphertext.
- **Ciphertext** (or **cipher text**, **encrypted text**, ...): transformed (or "scrambled", ...) text that needs to be "processed" to be "understood" (e.g., by a human being).
- **Decryption**: transformation (or function, process, procedure, ...) D that takes in input a ciphertext and a key and generates a plaintext.

Cipher: a function (or algorithm, ...) for performing encryption/decryption.

General cryptographic schema



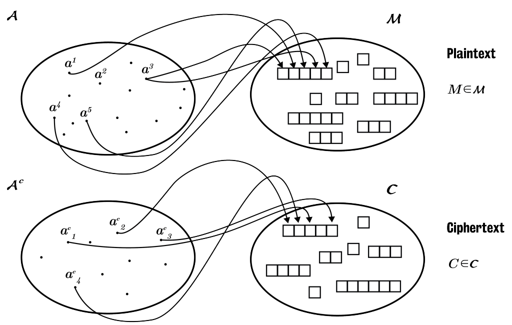
where $E(Key_1, P) = C$ and $D(Key_2, C) = P$.

- **Symmetric algorithms**:
  - $Key_1 = Key_2$, or are easily derived from each other.
- **Asymmetric (or public key) algorithms**:
  - Different keys, which cannot be derived from each other.
  - Public key can be published without compromising private key.
- Encryption and decryption should be easy, if keys are known.
- **Security depends only on secrecy of the key, not on the algorithm.**

A mathematical formalization of encryption/decryption

- $\mathcal{A}$, the alphabet, is a finite set.
- $\mathcal{M} \subseteq \mathcal{A}^*$ is the message space. $M \in \mathcal{M}$ is a plaintext (message).
- $\mathcal{C}$ is the ciphertext space, whose alphabet may differ from $\mathcal{M}$.
- $\mathcal{K}$ denotes the key space of keys.
- Each $e \in \mathcal{K}$ determines a bijective function from $\mathcal{M}$ to $\mathcal{C}$, denoted by E_e. E_e is the encryption function (or transformation).

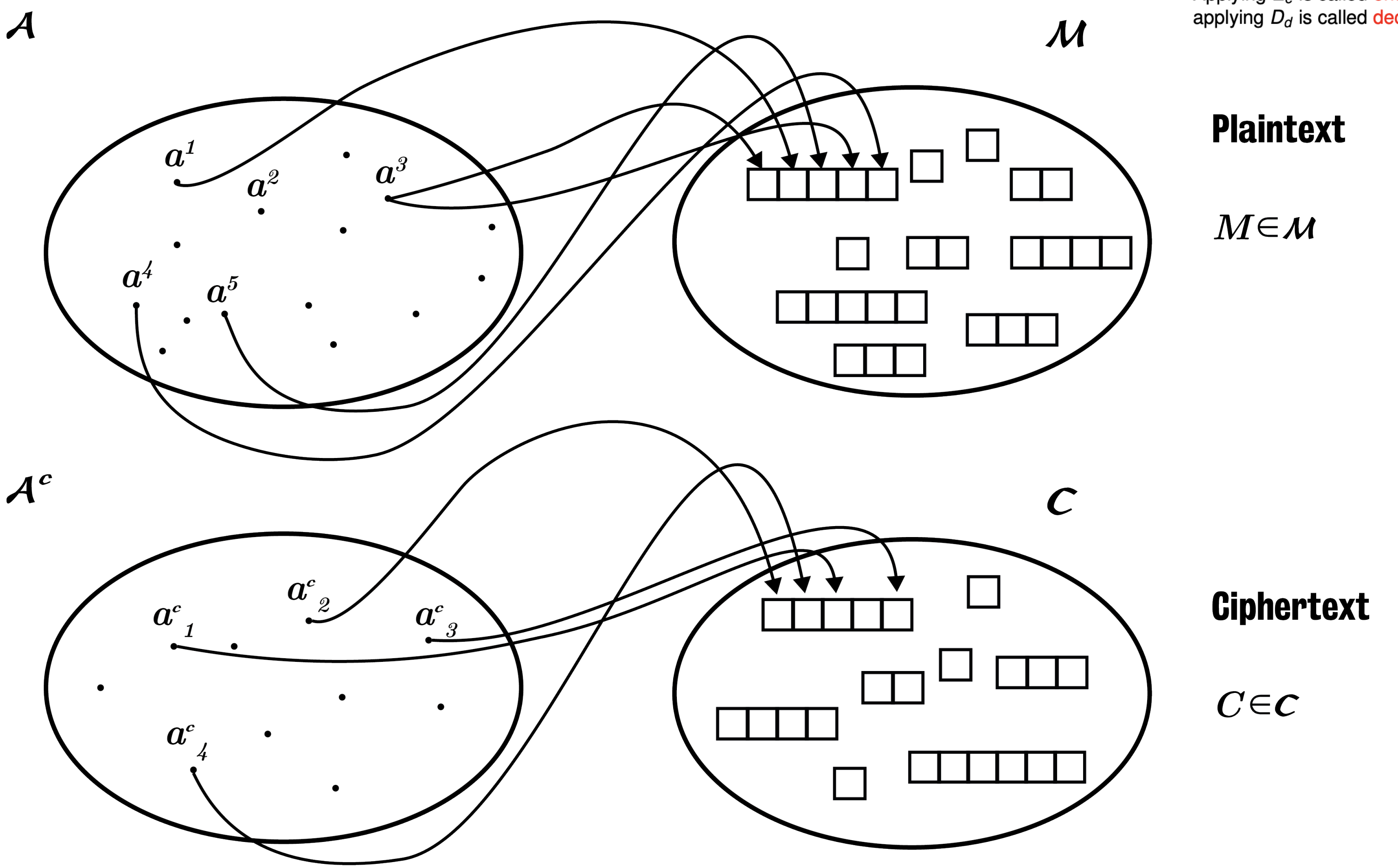
  Note: we will write $E_e(P) = C$ or, equivalently, $E(e, P) = C$.
- For each $d \in \mathcal{K}$, D_d denotes a bijection from $\mathcal{C}$ to $\mathcal{M}$. D_d is the decryption function.
- Applying E_e is called encryption, applying D_d is called decryption.



A mathematical formalization of en-/decryption (cont.)

- $\mathcal{A}$, the alphabet, is a finite set.
- $\mathcal{M} \subseteq \mathcal{A}^*$ is the message space. $M \in \mathcal{M}$ is a plaintext (message).
- $\mathcal{C}$ is the ciphertext space, whose alphabet may differ from $\mathcal{M}$.
- $\mathcal{K}$ denotes the key space of keys.
- Each $e \in \mathcal{K}$ determines a bijective function from $\mathcal{M}$ to $\mathcal{C}$, denoted by E_e. E_e is the encryption function (or transformation).

  Note: we will write $E_e(P) = C$ or, equivalently, $E(e, P) = C$.
- For each $d \in \mathcal{K}$, D_d denotes a bijection from $\mathcal{C}$ to $\mathcal{M}$. D_d is the decryption function.
- Applying E_e is called encryption, applying D_d is called decryption.



A mathematical formalization of en-/decryption (cont.)

- An encryption scheme (or cipher) consists of a set $\{E_e \mid e \in \mathcal{K}\}$ and a corresponding set $\{D_d \mid d \in \mathcal{K}\}$ with the property that for each $e \in \mathcal{K}$ there is a unique $d \in \mathcal{K}$ such that $D_d = E_e^{-1}$; i.e.,

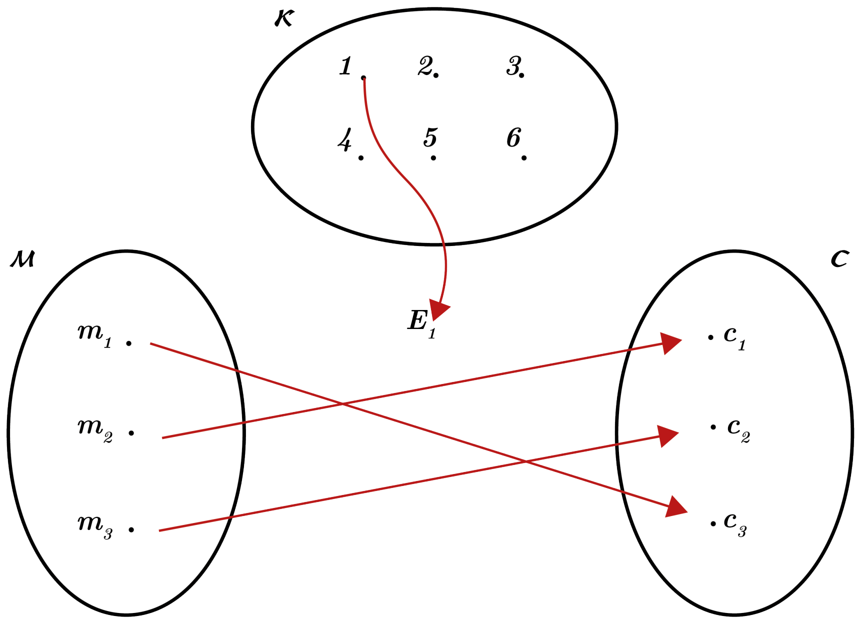
$$D_d(E_e(m)) = m \qquad \text{for all } m \in \mathcal{M}\,.$$

- The keys e and d above form a key pair, sometimes denoted by (e, d). They can be identical (i.e., the symmetric key).

- To construct an encryption scheme requires fixing a message space $\mathcal{M}$, a ciphertext space $\mathcal{C}$, and a key space $\mathcal{K}$, as well as encryption transformations $\{E_e \mid e \in \mathcal{K}\}$ and corresponding decryption transformations $\{D_d \mid d \in \mathcal{K}\}$.

An example

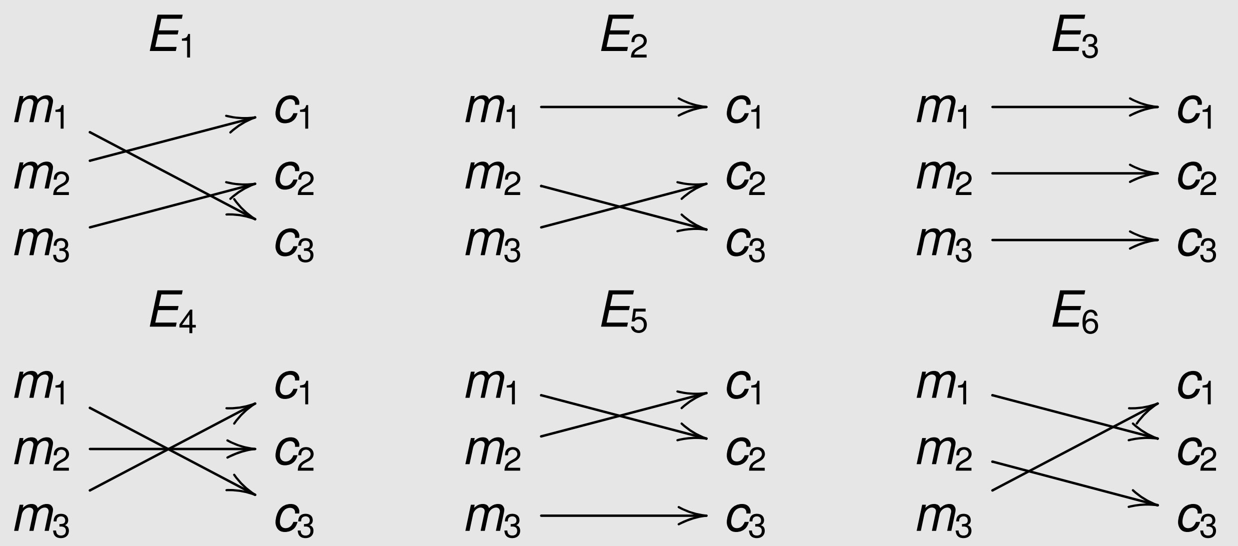
Let $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{C} = \{c_1, c_2, c_3\}$.
There are 3! = 6 bijections from $\mathcal{M}$ to $\mathcal{C}$.
The key space $\mathcal{K} = \{1, 2, 3, 4, 5, 6\}$ specifies these transformations.



Suppose Alice and Bob agree on the transformation E_1.
To encrypt m_1, Alice computes $E_1(m_1) = c_3$.
Bob decrypts c_3 by reversing the arrows on the diagram for E_1 and observing that c_3 points to m_1.

An example (cont.)

Let $\mathcal{M} = \{m_1, m_2, m_3\}$ and $\mathcal{C} = \{c_1, c_2, c_3\}$.
There are 3! = 6 bijections from $\mathcal{M}$ to $\mathcal{C}$.
The key space $\mathcal{K} = \{1, 2, 3, 4, 5, 6\}$ specifies these transformations.



Suppose Alice and Bob agree on the transformation E_1.
To encrypt m_1, Alice computes $E_1(m_1) = c_3$.
Bob decrypts c_3 by reversing the arrows on the diagram for E_1 and observing that c_3 points to m_1.