Cryptography – Exam Questions

Tim Herbstrith

2020

Contents

1 Cryptography principles / Basic model for secrecy / Cryptosystem for secrecy

Cryptography principles definitions, (non) examples. Basic cryptography concepts (primitive, protocol, cover time, etc.). Basic model for secrecy: (non)-examples. Cryptosystem for secrecy: definition, examples. Symmetric versus asymmetric cryptosystems.

1.1 Cryptography principles

- Confidentiality / secrecy:
  - limit access to information
- Data Integrity
  - data was not altered (intentionally or accidentally)
  - detection of alteration (not prevention)
- Data origin authentication / message authentication
  - confirms the origin of data with no temporal aspect to the **receiver**
  - not necessarily an immediate source / not when
- Entity authentication

  - a given entity is involved and currently active
  - e.g. log in at web service
- Non-Repudiation
  - a source of data cannot deny to a **third party** being at the origin

Data origin authentication $\Rightarrow$ Data integrity

Non-Repudiation $\Rightarrow$ Data origin authentication

Data origin authentication $\neq$ Entity authentication

Secrecy $\nRightarrow$ Data origin authentication

1.2 Different cryptographic concepts

- Cryptography = **toolkit**
- Cryptographic **primitive** = a basic tool in this toolkit
  - Examples: Encryption, hash function, MAC (message authentication code), digital signature, etc.
- Cryptographic **algorithm** = Cipher = a specification of a primitive
- Cryptographic **protocol** = a way to choose primitives and use them for a security goal
- Crypto**system** = implementation of primitives and the infrastructure

1.3 Basic model of a cryptosystem

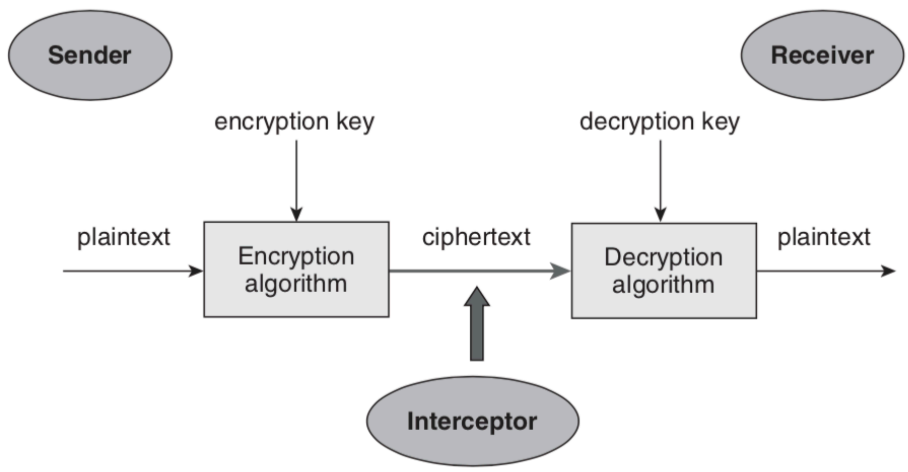

Figure 1: Basic model of a cryptosystem (Martin 2012)

Fig. 1 depicts a sender who wishes to transfer some data to a receiver in such a way that any party intercepting the transmitted data cannot determine the content. *The interceptor must not know the decryption key.*

Secrecy can be provided by (combination of):

1. Cryptography (via encryption)
2. Steganography (via information hiding)

3. Access control (via software or hardware)

1.4 Definition of Cryptosystem

Cryptosystem is a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ satisfying:

- $\mathcal{P}$ is a finite set of possible **plaintexts**;
- $\mathcal{C}$ is a finite set of possible **ciphertexts**;
- $\mathcal{K}$, the keyspace, is a finite set of possible **keys**;
- $\mathcal{E} = \{E_k : k \in \mathcal{K}\}$ consists of **encryption functions** $E_k : \mathcal{P} \to \mathcal{C}$;
- $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ consists of **decryption functions** $D_k : \mathcal{C} \to \mathcal{P}$;
- For all $e \in \mathcal{K}$ there exists $d \in \mathcal{K}$ such that for all plaintexts $p \in \mathcal{P}$ we have:
$$D_d(E_e(p)) = p$$

The cryptosystem is

- **symmetric** if $e = d$ and
- **public-key** if d cannot be derived from e in a computationally feasible way

1.5 Cover time

Cover time = the time for which a plaintext must be kept secret.

2 Attacks on encryption algorithms

Main attacks on encryption algorithms. Passive versus active attacks. Keys: length, size. Brute-force attack: assumptions, estimates on key lengths.

2.1 Targets of attacks

- A practical method of determining the **decryption key** is found.
- A weakness in the encryption algorithm leads to a **plaintext**.

2.2 Passive vs active attacks

- The main type of **passive attack** is unauthorised access to data.
- An **active attack** involves either data being changed in some way, or a process being conducted on the data.

2.3 Key lengths and sizes

- **Length** of the key = number of bites it takes to represent the key
- **Size** of the keyspace = number of possible different decryption keys

2.4 Assumptions

- All keys from the keyspace are equally likely to be selected
- The correct decryption key is identified as soon as it is tested

2.5 Estimates on key length

If Size $= n = 2k$, then, on average, one needs $\sim 2k - 1$ attempts to find the correct decryption key:

$$\mathbb{E}[X] = \sum_{i=1}^{n} i\frac{1}{n} = \frac{n\,(n-1)}{2} = \frac{2^k+1}{2} \sim 2^{k-1}$$

. . .

References

Martin, Keith M. 2012. *Everyday Cryptography: Fundamental Principles and Applications*. Oxford University Press.