

Cryptography – Exam Questions

Tim Herbstrith

2020

Contents

1	Cryptography principles / Basic model for secrecy / Cryptosystem for secrecy	2
2	Attacks on encryption algorithms	4
3	Examples of symmetric cryptosystems	5
4	Computational complexity	5
5	Three types of security	5
6	RSA cryptosystem	5
7	One-way functions	5
8	Hash functions	5
9	Discrete logarithm problem	5
10	ElGamal cryptosystem	5
11	Elliptic curves	6
12	Group structure on elliptic curves	6
13	Cayley-Bacharach's theorem	6
14	Associativity	6
15	Elliptic curves over finite fields	6
16	Diffie-Hellman key agreement protocol	6
17	Digital signature scheme	6
18	DSS with hashing	8
19	DSS and Public-key cryptosystems	9

20 ElGamal variant of DSS (Definition)	9
21 ElGamal variant of DSS (Misuse)	9
22 Digital currency	9
23 Bitcoin transactions	9
24 Bit generators	9
25 Distinguisher and next bit predictors	9
26 Error-correcting codes and expander graphs	10
27 Probabilistic pidgeonhole principle	10
28 Attacks on cryptosystems relying on structural weaknesses	10
29 Shanks algorithm	10

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
- Cryptosystem = implementation of primitives and the infrastructure

1.3 Basic model of a cryptosystem

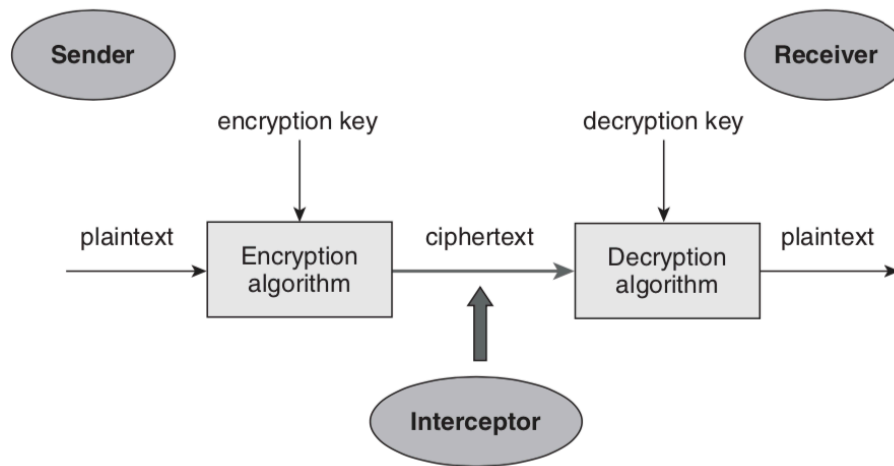


Figure 1: Basic model of a cryptosystem (Martin 2012)

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** $E_k : \mathcal{P} \rightarrow \mathcal{C}$;
- $\mathcal{D} = \{D_k : k \in \mathcal{K}\}$ consists of **decryption functions** $D_k : \mathcal{C} \rightarrow \mathcal{P}$;

- 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:

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

3 Examples of symmetric cryptosystems

Examples of symmetric cryptosystems: Caesar and Substitution ciphers. The letter frequency analysis. Monoalphabetic and polyalphabetic cyphers. Vigenère cipher. If the given key of a Vigenère Cipher has repeated letters, does it make it any easier to break?

4 Computational complexity

Computational complexity of basic mathematical operations and of the exhaustive key search attack. Complexity classes of algorithms.

5 Three types of security

Three types of security. Perfect secrecy: definition, examples, equivalent formulations (with proof). Perfect secrecy: Shannon's Theorem (with proof).

6 RSA cryptosystem

RSA cryptosystem: definition, examples, correctness (encryption and decryption are inverse operations). Parameter generation, its complexity. Main attacks.

7 One-way functions

One-way function, with trapdoor. Theorem: RSA keys vs Factoring (formulation and sketch of proof).

8 Hash functions

Hash function: definition, types of resistance, (non)-examples. Optimal asymmetric encryption padding.

9 Discrete logarithm problem

Discrete logarithm problem. The DLP assumption. The DLP in $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ Is breaking the ECC cryptosystem equivalent to solving the DLP?

10 ElGamal cryptosystem

ElGamal cryptosystem and parameter generation: definition, correctness (encryption and decryption are inverse operations). Theorem: ElGamal keys versus DLP (with proof).

11 Elliptic curves

Elliptic curve: definition, singularities, normal forms, tangents. Theorem: intersection of E with a projective line (with proof).

12 Group structure on elliptic curves

Group structure on the elliptic curve over the algebraic closure, geometrically: definition and theorem (with proof).

13 Cayley-Bacharach's theorem

Cayley-Bacharach's theorem (with proof).

14 Associativity

Associativity (sketch of proof).

15 Elliptic curves over finite fields

Elliptic curves over finite fields: theorems (without proof) and examples. Check that for a prime q , each natural number in the Hasse interval occurs as the order of the elliptic curve group over the field of q elements.

16 Diffie-Hellman key agreement protocol

Diffie-Hellman key agreement: protocol, attacks. The DHP problem. The ECDHE.

17 Digital signature scheme

Digital Signature Scheme. RSA signature algorithm. Attacks: definitions and examples.

To ensure the **non-repudiation** of data

17.1 Definition

Signature scheme is a 5-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, satisfying:

- \mathcal{P} is a finite set of possible **messages**;
- \mathcal{A} is a finite set of possible **signatures**;
- \mathcal{K} , the keyspace, is a finite set of possible **keys**;
- $\mathcal{S} = \{sig_k : k \in \mathcal{K}\}$ consists of polynomial signing algorithms $sig_k : \mathcal{P} \rightarrow \mathcal{A}$;

- $\mathcal{V} = \{ver_k : k \in \mathcal{K}\}$ consists of polynomial verification algorithms $ver_k : \mathcal{P} \times \mathcal{A} \rightarrow \{\mathbf{true}, \mathbf{false}\}$;

$$\forall x \in \mathcal{P}, \forall y \in \mathcal{A} : ver_k(x, y) = \begin{cases} \mathbf{true}, & \text{if } y = sig_k(x) \\ \mathbf{false}, & \text{otherwise} \end{cases}$$

A pair (x, y) with $x \in \mathcal{P}$, $y \in \mathcal{A}$ is called a **signed message**.

17.2 RSA signature algorithm

Public-key cryptosystem	Digital Signature
Encrypt with E_k	Sign with D_k
Decrypt with D_k	Verify with E_k

RSA signature scheme is a 5-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ such that:

- $n = pq$, where p, q are primes,
- $\mathcal{P} = \mathcal{A} = \mathbb{Z}/n\mathbb{Z}$, and
- $\mathcal{K} = \{(n, p, q, d, e) : de = 1 \pmod{\phi(n)}\}$
- For $k = (n, p, q, d, e)$, we define

$$sig_k(x) = x^d \pmod{n} \quad \text{and}$$

$$ver_k(x, y) = \begin{cases} \mathbf{true}, & \text{if } x = y^e \pmod{n} \\ \mathbf{false}, & \text{otherwise.} \end{cases}$$

- Public-key is (n, e) and private-key is (p, q, d) .

Note: By the definition of DSS we should have:

$$\begin{aligned} ver_k(x, y) = \mathbf{true} &\Leftrightarrow y = sig_k(x) = x^d \pmod{n} \\ &\Leftrightarrow x = y^e \pmod{n} \end{aligned}$$

Since $de = 1 \pmod{\phi(n)}$, we have $de = t\phi(n) + 1$ for some $t \in \mathbb{Z}$. If $x \in (\mathbb{Z}/n\mathbb{Z})^*$, then

$$\begin{aligned} (x^e)^d &= x^{t\phi(n)+1} \pmod{n} = (x^{\phi(n)})^t x \pmod{n} = \\ &\stackrel{|\mathbb{Z}/n\mathbb{Z}|^* = \phi(n)}{=} 1^t x \pmod{n} = x \pmod{n} \end{aligned}$$

If $x \notin (\mathbb{Z}/n\mathbb{Z})^*$, we know that $x \equiv 0 \pmod{p}$ or $x \equiv 0 \pmod{q}$ and uses Fermat's little theorem and the Chinese remainder theorem as in sec. 6.

17.3 Attacks on DSS

- **Key-only:** The attacker knows the public verification key, hence, ver_k .
- **Known message:** The attacker knows some messages (not selected by him) and their signatures.

- **Chosen message:** The attacker knows some messages (selected by him) and their signatures.

17.4 Goals of attacks on DSS

- **Total break:** The attacker determines Alice's private key, hence, sig_k .
- **Selective forgery:** With a non-negligible probability, the attacker creates a valid signature on a message chosen by someone else.
- **Existential forgery:** Forge a signature for some message (without the ability to do this for any message).
- **Universal forgery:** Forge signatures of any message.

17.5 Examples of attacks

1. *Existential forgery using key-only attack* is always possible: Choose an arbitrary signature y , then compute the message x given by $x := E_k(y)$.
 \Rightarrow use **redundancy** or **hashing**.
2. *Universal forgery under a chosen message attack* is possible, if one-way function with trapdoor is multiplicative (e.g. RSA $(xy)^e = x^e \cdot y^e$). To sign $x = x_1 x_2$ trick Alice into signing x_1, x_2 to obtain y_1, y_2 and compute $(x, y) = (x, y_1 y_2)$.

18 DSS with hashing

DSS with hashing. Hash functions from block ciphers: definition and example, with proof (the example where $(x, y) \rightarrow a^x b^y$).

DSS + Hashing = Hash-then-sign

18.1 Definition

DSS with hashing is a DSS 5-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ such that:

- $\mathcal{P} = \{0, 1\}^*$ and
- $\mathcal{A} = \{0, 1\}^l$ for some $l \in \mathbb{N}$;
- $h : \mathcal{P} \rightarrow \mathcal{A}$ a public **hash function** given by a polynomial algorithm;
- $sig_k(x) = f_k^{-1}(h(x))$, where $f_k : \mathcal{A} \rightarrow \mathcal{A}$ is a one-way function with trapdoor.
- $\forall x \in \mathcal{P}, \forall y \in \mathcal{A} : ver_k(x, y) = \begin{cases} \text{true}, & \text{if } f_k(y) = h(x) \\ \text{false}, & \text{otherwise.} \end{cases}$

To avoid the attacks h must be a one-way **non-multiplicative** function. h is **collision resistant** if it is infeasible to find $x_1 \neq x_2$ with $h(x_1) = h(x_2)$.

A **block cipher** encodes blocks of bits at a time (e.g. Vigenère, Feistel).

18.2 Definition

Hash functions from block ciphers:

Let $\mathcal{P} = \mathcal{K} = \mathcal{C} = \{0, 1\}^l$ for some $l \in \mathbb{N}$ and E be a block cipher:

$$E : \mathcal{P} \times \mathcal{K} \rightarrow \mathcal{C}, \quad (x, e) \mapsto E_e(x).$$

Define $h(x_1, \dots, x_r) \in \{0, 1\}^l$ with $x_i \in \{0, 1\}^l$ recursively (on r), by $h(\emptyset) = 0$, and

$$h(x_1, \dots, x_r) = E_{e_h}(x_r) + e_h, \text{ where } e_h = h(x_1, \dots, x_{r-1}).$$

SHA-1 is an example of such a hash function.

19 DSS and Public-key cryptosystems

DSS and Public-key cryptosystem: sign-then-encrypt versus encrypt-versus-sign.

20 ElGamal variant of DSS (Definition)

ElGamal variant of DSS: definition and correctness. Security assumptions. Example of misuse (with proof).

21 ElGamal variant of DSS (Misuse)

ElGamal variant of DSS: example of misuse (with proof). ECDSA: definition and correctness.

22 Digital currency

Digital currency: definition and security requirements. Distributed ledgers. Blockchain. Security assumptions underlying the generation of the bitcoin address.

23 Bitcoin transactions

Bitcoin transaction and its verification. Merkle tree. Bitcoin mining.

24 Bit generators

Bit generator. Linear feedback shift register: definition, periods, security. RSA bit generator.

25 Distinguisher and next bit predictors

Distinguisher. Next bit predictor. Yao's theorem (sketch of proof).

26 Error-correcting codes and expander graphs

Error-correcting codes and expander graphs

27 Probabilistic pidgeonhole principle

Describe the probabilistic pidgeonhole principle and explain, with examples, why it is relevant in cryptography (i.e hash functions, birthday paradox etc).

28 Attacks on cryptosystems relying on structural weaknesses

Describe a variety of attacks that rely on structural weaknesses in respective cryptosystems (for instance, known message attacks for multiplicative systems, or weaknesses of El Gamal under weak random choices).

29 Shanks algorithm

Describe Shanks algorithm, give examples of its use and outline how to use Shanks Algorithm to compute the order of an elliptic curve of prime order in combination with Hasse's bound.

References

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