

Data privacy: Exercises

October 1, 2026

1 RSA

Exercise 1 For encryption purposes, the receiver Bob chooses RSA encryption system with $p = 3$ and $q = 11$, two prime numbers. Describe

- the key generation process by Bob
- the RSA protocol (encryption and decryption).

Exercise 2 Consider the RSA cryptosystem with the public key $(n = 55, e = 27)$. It has been revealed that $(p - 1) \times (q - 1) = 40$. Use this information to

- find the secret key d ,
- factor n .

Exercise 3 Alice, the sender, decides to use RSA signature protocol with $p = 3$ and $q = 11$. Describe

- the signature key generation process by Alice
- the RSA signature protocol.

Exercise 4 For using RSA cryptosystem Alice chooses $p = 5$ and $q = 11$ two prime numbers, and the public key $(n, e) = (55, 27)$. Use this information to

- find the Alice secret key d ,
- describe the RSA encryption protocol.

Exercise 5 Alice publishes the following data $n = pq = 21$ and $e = 5$. Bob receives the message $P = 2$ and the corresponding digital signature $S = 11$.

Question: Verify the signature.

2 Diffie-Hellman

Exercise 6 Assume that two users want to establish a common secret key over an insecure channel by using Diffie-Hellman key exchange protocol. The private key for user A is 3 and for user B is 5. We consider a commonly known prime 11.

Question:

- (i) Find the smallest primitive element (that is, generator) for $p = 11$ (Show your steps).
- (ii) Obtain the common key by using the primitive element found above. (Show your steps. Draw a sequence diagram with all the messages, using the specific values given above, exchanged between the two.)

Exercise 7

- Calculate $2^9 \bmod 11$
- Find x such that $2^x = 5 \bmod 11$; and y such that $2^y = 3 \bmod 11$
- Show that 2 is a generator of F_{11}
- Provide details of the Diffie-Hellman key exchange protocol with the prime number $p = 11$ and the generator $g = 2$.

3 ElGamal

Exercise 8 The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange.

The algorithm:

- Alice (the receiver) and Bob (the sender) agree, on a public channel, on p a great prime number and g , a generator of F_p
- Alice chooses an integer a randomly from $\{1, 2, \dots, p-1\}$; computes $A = g^a \bmod p$; and sends A to Bob
- Bob chooses an integer b randomly from $\{1, 2, \dots, p-1\}$; computes $B = g^b \bmod p$; and sends B to Alice
- Bob wants to send the message m , an integer in $\{1, 2, \dots, p-1\}$ to Alice. He computes $C = m \cdot A^b$, and sends C to Alice (C is encrypted version of m)
- Alice decrypts C : she computes $B^{p-1-a} \cdot C$, which is equal to m .

Exercise 9 Describe the ElGamal algorithm

- when the public key is $p = 5$, $g = 2$
- the secret key of Alice is $a = 2$ and that of Bob $b = 3$
- the secret message of Bob is $m = 4$.

4 Cryptographic Hash function

Exercise 10 Explain the purpose of the collision-resistance requirement for the hash function used in a digital signature scheme.

Exercise 11 (collision for hash function) Consider the uniform distribution of birthdays in a 365-day year.

A. What is the probability that *two people in a group have a birthday on the same day* if the group consists of

1. 2 people,
2. 23 people,
3. 97 people.

Answer: 1: $\approx 3 \cdot 10^{-3}$; 2: ≈ 0.507 ; 3: ≈ 0.99999992 . We can see that while it is very improbable for two people to have birthday on the same day, for only 23 people we have over 50% chance that there are two people with birthday on the same day. For 97 people it is almost certain there will be such a pair.

B. Same question if you require that *at least 1 person has a particular birthday* (say, the 15th of February), if the group consists of

1. 2 people,
2. 23 people,
3. 97 people,
4. 253 people.

Answer: 1: ≈ 0.0054 ; 2: ≈ 0.0611 ; 3: ≈ 0.06115 ; 4: ≈ 0.50047 .

5 Shamir's Secret Sharing

Exercise 12 Let's imagine that a family of four members all share a single Bitcoin wallet. This Bitcoin wallet contains a single private key that all members of the family co-own. Because there is a single key, any of the family members can use that key to spend all of the Bitcoins.

The family has a problem: If each of them keeps a copy of the key, then only one of the copies is enough to be compromised to have all the coins stolen. If only one of them keeps the key, then that person may lose it or decide to double-cross the other family members.

Luckily, one of the family members is also a cryptographer. Instead of naively sharing the original key, they use Shamir's secret sharing. The family creates four shares and sets a threshold of three, with the Bitcoin key as the original secret. Now, their plan has the following properties:

- They have not stored the bitcoin key in a single place which makes it harder to steal
- Members of the family need to cooperate to spend the Bitcoin, one family member can't betray the others
- If a family member dies or loses their share, the other three members can still reconstruct the key.

Question: Explain how they can realise their plan.

Exercise 13 A four people family decides to keep their fortune in a digital locked safe. Each people has its own PIN code. The safe opens if any two among the four people enter their PIN code. The codes are:

$$P1: 2 \quad P2: 5 \quad P3: 8 \quad P4: 0$$

- Give the corresponding polynomial $f(x)$
- Compute the secrete $f(0)$

All calculations will be made modulo 11.

Exercise 14 A military office consists of one General, two Colonels and five Majors. They have control of a powerful missile, but they do not want to launch it unless

- the General decides to launch it, or
- two Colonels decide to launch it, or
- five Majors decide to launch it, or
- one Colonel together with three Majors decide to launch it.

How they would do that with a secret sharing scheme.

Exercise 15 A four people family decides to keep their fortune in a digital locked safe. Each people has its own PIN code. The safe opens if any two among the four people enter their PIN code. The codes are:

$$P1: 2 \quad P2: 5 \quad P3: 8 \quad P4: 11$$

- Give the corresponding polynomial $f(x)$
- Compute the secrete $f(0)$

6 Authentication

Exercise 16 Alice and Bob have a shared secret k and have decided to use it in the following protocol, which enables Alice to identify Bob as the party at the other end.

1. Alice picks a random string r and sends it as challenge to Bob.
2. Bob responds with $r \oplus k$.

Alice's and Bob's analysis of the protocol is this: The protocol does indeed provide identification, since Alice can check that the sender of message 2. knows k . It is also secure, since only random numbers are ever sent on the communication channel.

Question: How does Alice check that the sender of message 2. knows k .