Fundamentals

Exercises

1. Let $X = ([-1, 1] \cap \mathbb{Z}) \times \{0, 1\}$.
   (a) Enumerate the elements of X and determine $|X|$.
   (b) Let $Y = \{1, 2, \ldots, |X|\}$. Give an explicit bijection from X to Y.
2. Which of the following maps are *injective*, *surjective* or *bijective*? Determine the image $im(f)$ and give the inverse map f^{-1}, if possible.
   (a) $f_1 : \mathbb{N} \to \mathbb{N}$, $f_1(n) = 2n + 1$
   (b) $f_2 : \mathbb{Z} \to \mathbb{N}$, $f_2(k) = |k| + 1$
   (c) $f_3 : \{0, 1\}^8 \to \{0, 1\}^8$, $f_3(b) = b \oplus (01101011)$
   (d) $f_4 : \{0, 1\}^8 \to \{0, 1\}^8$, $f_4(b) = b$ AND (01101011)
3. Let $f : X \to Y$ be a map between finite sets and suppose that $|X| = |Y|$. Show the following equivalences:

$$f \text{ is injective } \iff f \text{ is surjective } \iff f \text{ is bijective}$$

4. Let $f : X \to Y$ be a function.
   (a) Let $B \subset Y$. Show that $f(f^{-1}(B)) \subset B$ with equality occurring if f is surjective.
   (b) Let $A \subset X$. Show that $A \subset f^{-1}(f(A))$ with equality occurring if f is injective.
5. Enumerate the integers modulo 26. Find the standard representative of the following integers in $\mathbb{Z}_{26}$:

$$-1000,\ -30,\ -1,\ 15,\ 2001,\ 293829329302932398231$$

6. Find an asymptotic upper bound of the following functions in n. Which of them are polynomial and which are negligible?
   (a) $f_1 = 2n^3 - 3n^2 + n$

(b) $f_2 = 3 \cdot 2^n - 2n + 1$
(c) $f_3 = \sqrt{2n+1}$
(d) $f_4 = \frac{3}{2^{n/2}}$
(e) $f_5 = \frac{5n^2-n}{2n^3+3n+1}$
(f) $f_6 = 2^{\frac{1}{3}n+3}$
(g) $f_7 = \log_2(n)^2 + n$

7. Suppose the number of operations of the most efficient attack against a cipher is
$$f(n) = e^{\left(2n^{1/3}\right)}$$
where n is the key length. Why is $f(n)$ sub-exponential, but not polynomial in n? Compute the *effective key length* $\log_2(f(n))$ for $n = 128$, $n = 1024$ and $n = 2048$.

8. Let $\Omega = \{0,1\}^8$ be a probability space with a uniform probability distribution. Compute the probability that a randomly chosen byte is balanced, i.e., contains four zeros and four ones.

9. Two perfect dice are rolled and the random variables, which give the numbers on the dice, are called X and Y. Compute
$$Pr[X + Y \geq 10] \text{ and } Pr[X + Y \geq 10 \mid X - Y = 0]\,.$$
Are the random variables $X + Y$ and $X - Y$ independent? Determine the expectation, the variance and the standard deviation of $X + Y$ and $X - Y$.

10. Suppose that 100 bits are generated uniformly at random and additional bits are produced by XORing the preceding 100 bits. Are the new bits uniformly distributed? Does this construction give a random bit generator?

11. Which of the following residue classes are identical in $\mathbb{Z}_{26}$?
$$\overline{0},\ \overline{3},\ \overline{-49},\ \overline{49},\ \overline{104}$$

12. Enumerate the elements of $\mathbb{Z}_{22}^*$ and give $\varphi(22)$. Find the inverse of each element in $\mathbb{Z}_{22}^*$.

13. Use the Extended Euclidean Algorithm to compute the multiplicative inverse of $\overline{32} \in \mathbb{Z}_{897}^*$.

14. Let $p \neq q$ be prime numbers. Show that $\varphi(pq) = (p-1)(q-1)$.

15. Let p be a prime number and $m \in \mathbb{N}$. Find $\varphi(2p)$, $\varphi(2^m)$ and $\varphi(p^m)$.

16. Let $N = pq$, where p and q are different secret prime numbers. Then we have $\varphi(N) = (p-1)(q-1)$. Let A be the problem to factor N into p and q, and let B be the problem to compute $\varphi(N)$ given N. Show that there is a polynomial time reduction $A \leq_p B$.
Hint: Given N and $\varphi(N)$, compute $p+q$, express q by p and set up a quadratic equation in the unknown variable p.

17. Compute $2^{55} \mod 61$ using fast exponentiation. How many modular squarings and multiplications are necessary?

18. Determine the maximum number of modular squarings and multiplications that are needed to compute $x^k \mod n$ if $\text{size}\,(n) = \text{size}\,(k) = 2048$.

19. Give the entropy of 128 independent bits, where for each bit $p(0) = \frac{3}{4}$ and $p(1) = \frac{1}{4}$.
20. Give the entropy of n uniformly distributed octal numbers, i.e., n numbers 0 through 7. How many octal numbers are needed to achieve 80 bits of entropy?
21. Let Ω be a set of cardinality 1000 having a uniform distribution. How many randomly drawn samples are likely to produce a collision?

Encryption Schemes and Definitions of Security

Exercises

1. Show that the Vigenère cipher is perfectly secure if the key is randomly chosen, only used once and the plaintext has the same length as the key.
2. Find reasons for Kerkhoff's principle and discuss possible counter-arguments.
3. Show that the one-time pad is not perfectly secret if a key is used twice.
4. Let $\mathcal{M}$ be the plaintext space and $\mathcal{K}$ the key space of a perfectly secure encryption scheme. Show that $|\mathcal{K}| \geq |\mathcal{M}|$.
   Hint: Suppose $\mathcal{E}_k(m_0) = c$. How many different plaintext-key pairs give the ciphertext c?
5. Is a bit permutation of block length n perfectly secure if it is used only once to encrypt a string of length n?
6. Suppose an encryption scheme with security parameter n can be broken with a probability of $\frac{1}{n^2}$ after $2n^5$ computing steps. Give the concrete computational security for $n = 256$. Is the scheme computational secure?
7. Explain the differences in the definitions of EAV-secure and CPA-secure encryption schemes.
8. Prove that a perfectly secure scheme is EAV-secure. Show that $\mathrm{Adv}^{\mathrm{eav}}(A)$ is 0 for any adversary A. Why is perfect security much stronger than EAV security?
9. Does the Vigenère cipher (of fixed key-length) define an EAV-secure encryption scheme (for messages of arbitrary length)?
10. Suppose G is a pseudorandom generator with fixed output-length. Define an associated encryption scheme by $\mathcal{E}_k(m) = m \oplus G(k)$. Show that this scheme is not EAV-secure for multiple encryptions with the same key.
11. The success probability of an adversary in the CPA experiment against an encryption scheme is
    (a) $\frac{1}{2} + e^{-n}$,
    (b) $\frac{1}{2} + \frac{1}{n^3}$,
    where n is the key length. Does this contradict CPA security of the scheme?

12. Explain why a malleable encryption scheme, where it is possible to transform a ciphertext into another ciphertext which decrypts to a related plaintext, cannot be CCA2-secure.
13. Let F be a family of bit permutations, i.e., only the position of the bits changes. Is F a pseudorandom permutation?
14. Show that a block cipher in ECB mode is not EAV-secure.
15. Consider a block cipher in CBC mode. Suppose that the initialization vector IV is initially set to 0 and then incremented for every new encryption. Can this variant of the CBC mode be CPA-secure?
16. Why is a block cipher in CTR mode vulnerable to ciphertext-only attacks if the counter is re-used? Show that the CTR mode is not EAV-secure for multiple encryptions if the counter is re-used.
17. Can an encryption scheme that is based on a block cipher be perfectly secure?
18. Let E be a block cipher of block length 4 and suppose that $E_k(b_1b_2b_3b_4) = (b_2b_3b_4b_1)$. Encrypt $m = 1011\ 0001\ 0100$ and decrypt the ciphertext with the following operation modes:
    (a) ECB mode,
    (b) CBC mode with $IV = 1010$,
    (c) CTR mode with $ctr = 1010$.
19. Consider a block cipher in CBC mode. The ciphertext is sent to a receiver. What are the consequences, if:
    (a) the receiver misses the initialization vector (IV), or
    (b) a single ciphertext block is changed due to transmission errors, or
    (c) a ciphertext bit is flipped by an adversary during the transmission, or
    (d) a bit error occurs during the ciphering operation ?
20. Suppose a block cipher of block length 128 in CTR mode is used to encrypt 300 bits of plaintext. Which bits cannot be correctly decrypted if one of the following errors occurs?
    (a) The first bit of the counter value is flipped during transmission,
    (b) The first ciphertext bit is flipped,
    (c) The first ciphertext block c_1 is changed due to transmission errors,
    (d) The last ciphertext bit is flipped.
21. Compare ECB, CBC and CTR mode with respect to message expansion, error propagation, pre-computations and parallelization of encryption and decryption.
22. Explain why neither CBC nor CTR mode achieve CCA2 security.

Symmetric Ciphers

Exercises

1. Explain the difference between block and stream ciphers.
2. Consider a block cipher in CTR mode and the induced stream cipher. Is it necessary to keep the counter *ctr* secret? Let $i \in \mathbb{N}$. Is there a relationship between the key bits derived from $ctr + i$ and $ctr + i + 1$?
3. Why can you produce diffusion with linear maps (matrix operations) and adding round keys, but not confusion?
4. Why is it important that a Substitution-Permutation Network (SPN) has multiple rounds? How can you attack a SPN with only one round and no final key-mixing step?
5. Which are the diffusion and the confusion operations in AES?
6. Verify the following inverses in $GF(2^8)$ (in hexadecimal notation):

   $$\texttt{01}^{-1} = \texttt{01},\ \texttt{02}^{-1} = \texttt{8D},\ \texttt{03}^{-1} = \texttt{F6}$$

   Then compute $S_{RD}(\texttt{00})$, $S_{RD}(\texttt{01})$, $S_{RD}(\texttt{02})$ and $S_{RD}(\texttt{03})$.
7. Let $n \in \mathbb{N}$. Show that $f(x) = x^{(2^n)}$ is a $GF(2)$-linear map on $GF(2^8)$, whereas $f(x) = x^{254}$ is not linear.
8. Describe the inverse S-Box S_{RD}^{-1}.
9. Give a high-level (pseudocode) description of the AES decryption function f_k^{-1}.
10. Assume that a modified AES block cipher lacks all *ShiftRows* and *MixColumns* operations. Can this cipher be a pseudorandom permutation? What if only one of these operations is missing?
11. Suppose that the multiplicative inversion is omitted in the S-Box of a modified AES block cipher. Can this cipher be a pseudorandom permutation?
12. What is more important for a cipher: the non-linearity of encryption or the non-linearity of the key schedule?

Hash Functions

Exercises

1. Consider a hash function H. Explain why collision resistance implies second-preimage resistance.
2. Why are linear or affine hash functions not collision-resistant?
3. Why must the output of a collision-resistant hash function depend on *every* input bit?
4. Assume that a collision-resistant hash function is modified as described below. Is it still a collision-resistant hash function?
   (a) The low bit of the message is set to 1. The resulting message is hashed.
   (b) The low bit of the message is flipped, then the message is hashed.
   (c) All bits are flipped and then the message is hashed.
   (d) The message is split into blocks of a fixed length, the blocks are XORed and the result is hashed.
5. Give the probability that there is a collision in 10 randomly drawn numbers from a uniformly distributed set of 100 numbers.
6. (Birthday Paradox) Let Pr be a uniform distribution on the sample space Ω with $|\Omega| = n$. If $k \leq n$ samples are independently chosen, then the probability p that all k values are different (i.e., no collision occurs) is

$$p = \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right).$$

   (a) Show that the probability $1 - p$ of a collision satisfies

$$1 - p \geq 1 - e^{-\frac{k(k-1)}{2n}}.$$

   (b) Determine the smallest number k such that $p \approx \frac{1}{2}$.

   Hint: Use the inequality $1 - x \leq e^{-x}$ for $0 \leq x \leq 1$ and replace the factors $1 - \frac{i}{n}$ by $e^{-\frac{i}{n}}$. Compute the product and obtain a sum in the exponent. Use the formula $\sum_{i=1}^{k-1} i = \frac{k(k-1)}{2}$. For part (b), set $p = \frac{1}{2}$ and determine k using the quadratic formula. You may also approximate $k(k-1)$ by k^2. This gives the approximate number of samples needed for a probable collision.

7. Suppose we have an 80-bit hash function. How many hash values are likely to give a collision and why?
8. Consider a Merkle-Damgård hash function H. Show that an adversary, who knows a hash value $H(m)$ and the length of m, but not the input m, can generate an extended message M and compute the hash $H(M)$. This is called a *length extension attack*.
   Hint: Define M by concatenating m, the padding $10 \dots 0$, the encoded length L and any chosen message. Why can an adversary compute $H(M)$ without knowing m?
9. Find a reason why in the Merkle-Damgård construction the padded message includes the encoded length.
10. Why is the Sponge construction of SHA-3 not vulnerable to length extension attacks?

Message Authentication Codes

Exercises

1. What are possible reasons why a MAC is invalid?
2. Compare the properties of hashes and MACs when used for integrity protection.
3. Suppose a MAC does not depend on the first bit of the message. Why is such a MAC insecure under a chosen-message attack?
4. Show that appending the length L of a message does not turn the basic CBC MAC into a secure MAC for messages of variable length.
   Remark: In contrast, prepending a message with its length is secure.
5. Is it advisable to use the same key for CBC mode encryption and for CBC message authentication?
6. Show that $F_k(m) = H(k \,\|\, m)$ is not a secure MAC for Merkle-Damgård hash functions and arbitrary-length messages. Why is the HMAC construction not affected by this attack ?
7. In practice, HMAC-SHA1 and HMAC-SHA2 are often used as pseudorandom functions (prf). What is the rationale behind this choice?
8. Describe the computation of the GCM tag if the plaintext consists of one 128-bit block and AAD is empty.
9. A block cipher in CTR mode can only achieve CPA security. Describe a chosen ciphertext attack against the CTR mode and show that this attack is not possible if the CTR mode is combined with a secure MAC.

Algebraic Structures

Exercises

1. Let $L \subset \mathbb{R}^2$ be the following set:

$$L = \{(x, y) \in \mathbb{Z}^2 \mid x + y \equiv 0 \mod 2\}$$

   Show that L is an additive group and a lattice. Give a basis of L and sketch the lattice.

2. Find all subgroups of $(\mathbb{Z}_{10}, +)$, $(\mathbb{Z}_{11}, +)$ and $(\mathbb{Z}_{11}^*, \cdot)$.

3. Let G be a group of order 54. List the possible orders of elements in G.

4. Consider the map $f : (\mathbb{Z}_{19}, +) \to (\mathbb{Z}_{19}, +)$ defined by $f(x) = 5x \mod 19$. Show that f is a group homomorphism and even an isomorphism. Give the inverse homomorphism f^{-1}.

5. Let p and q be different prime numbers and $n = pq$. Let e and d be integers such that $ed \equiv 1 \mod (p-1)(q-1)$. Show that $m^{ed} \equiv m \mod n$ for any $m \in \mathbb{Z}_n$.
   Tip: Use Euler's Theorem to show the statement for $m \in \mathbb{Z}_n^*$.

6. Consider the multiplicative group $G = \mathbb{Z}_{23}^*$. Compute the order of $2 \mod 23$. What is the maximum order of elements in G? Find a generator of G.

7. Check whether $2 \mod 19$ and $5 \mod 19$ are generators of the multiplicative group $\mathbb{Z}_{19}^*$ and determine their order.

8. Show that $\mathbb{Z}_n \times \mathbb{Z}_n$ is not cyclic for $n \geq 2$.
   Tip: Verify that $\text{ord}(g) \mid n$ for all $g \in \mathbb{Z}_n \times \mathbb{Z}_n$.

9. Find all abelian groups of order 8, up to isomorphism. Which of them are cyclic?

10. Show that the multiplicative groups $\mathbb{Z}_{12}^*$ and $\mathbb{Z}_{23}^*$ are isomorphic to a product of additive cyclic groups and give their decompositions.

11. Which residue classes are generators of the *additive* group $\mathbb{Z}_n$?

12. Let $n = 247 = pq$. Find the factors p and q and solve the simultaneous congruences $k = 7 \mod p$ and $k = 2 \mod q$ using the Chinese Remainder Theorem.

13. Let R_1 and R_2 be rings. Why is the product ring $R_1 \times R_2$ never a field, even if R_1 and R_2 are fields?
    Tip: Consider the idempotent elements $(1, 0)$ and $(0, 1)$.
14. Determine the number of elements of the following residue class rings. Which of the rings are fields?
    (a) $GF(2)[x]/(x^4 + x^2 + 1)$
    (b) $GF(3)[x]/(x^2 + 1)$
    (c) $GF(p)[x]/(x^3 - 1)$, where p is a prime.
15. Let $R = GF(17)[x]/(x^2 - 4)$. Is R a field? Describe the elements of R and give explicit isomorphisms

    $$GF(17)[x]/(x^2 - 4) \longrightarrow GF(17)[x]/(x - 2) \times GF(17)[x]/(x + 2) \longrightarrow GF(17)^2$$

    Then give the inverse ring isomorphism

    $$GF(17)^2 \longrightarrow GF(17)[x]/(x^2 - 4).$$

    Hint: You need to find a polynomial $f(x)$ of degree < 2 with two given values $f(2)$ and $f(-2)$ modulo 17.
16. Let $GF(8) = GF(2)[x]/(x^3 + x + 1)$. Find representatives of x^3, x^4, x^5, x^6, x^7 in $GF(8)$ of degree less than 3.
17. Find an irreducible polynomial over $GF(2)$ of degree 6.
18. $GF(2^8)$ is the splitting field of $f(x) = x^{256} - x$, i.e., $GF(2^8)$ contains all roots of $f(x)$. Use SageMath to factor $f(x)$ over $GF(2)$ and identity the irreducible factor $g(x) = x^8 + x^4 + x^3 + x + 1$ used to define the AES field.
19. Define $GF(2^8)$ with $g(x)$ as in Exercise 18 above. Which polynomial $f(x)$ corresponds to the byte `02` (hexadecimal notation)? Find a polynomial $h(x)$ which is inverse to $f(x) \mod g(x)$, i.e. $f(x) \cdot h(x) \equiv 1 \mod g(x)$, and give its hexadecimal representation.

Public-Key Encryption and the RSA Cryptosystem

Exercises

1. Explain why a deterministic public-key encryption scheme is insecure if the number of possible plaintexts is small.

2. Suppose that p is a prime. Define a public-key scheme with the encryption function $\mathcal{E}_k(m) = m^e \mod p$ for a public key $k = (e, p)$ and a plaintext $m \in \mathbb{Z}_p^*$. Give the private key and the decryption function. Show that this scheme is insecure.

3. Consider a plain RSA cryptosystem with modulus $N = 437$ and public exponent $e = 5$.
   (a) Encrypt $m = 100$.
   (b) Factorize N and determine the private key d.
   (c) Decrypt the ciphertext and check that the result is $m = 100$.

4. Suppose that $m \in \mathbb{Z}_N$ is chosen uniformly at random, where $N = pq$ and $\text{size}(p) = \text{size}(q) = n$. Show that the probability of $m \notin \mathbb{Z}_N^*$ is negligible.

5. Bob's public RSA key is ($e = 35$, $N = 323$). Apply the plain RSA encryption scheme:
   (a) Encrypt the plaintext $m = 66$ with Bob's public key. Use the fast exponentiation method.
   (b) Mallory eavesdrops two ciphertexts $c_1 = 26$ and $c_2 = 213$, which were sent Bob, but he does not know the plaintexts m_1 and m_2. How can Mallory compute the ciphertexts corresponding to the plaintexts $m_1 m_2 \mod N$ and $m_1 m_2^{-1} \mod N$ without attacking RSA?
   (c) Mallory chooses $s = 5$ and computes $y = s^e \mod N \equiv 23$. He wants to find out the plaintext m corresponding to the ciphertext $c = 104$. He asks Bob to decrypt the 'innocent' ciphertext $c' = yc \mod N \equiv 131$ and gets the plaintext $m' = 142$. Why is Mallory now able to determine m without computing the private exponent d? Determine the plaintext m.
   (d) Now conduct an attack against the RSA key. Factorize N and compute d.

6. Side-channel attacks against RSA use the power consumption of an implementation to derive the private key. Suppose a microprocessor runs the square-and-multiply algorithm (see below) to decrypt a ciphertext with a private key d. An attacker analyzes the power trace and concludes that the decryption uses the following sequence of modular squarings (SQ) and multiplications (MULT): SQ, SQ, SQ, SQ, SQ, MULT, SQ, MULT, SQ, SQ, SQ, SQ, MULT, SQ, MULT.
   (a) Determine the private key d.
   (b) The public key is $(e = 11, N = 8051)$. Calculate $\varphi(N)$, p and q from d, e and N and verify your result.
7. The *Fermat primality test* of $n \in \mathbb{N}$ chooses a uniform random integer $a \in \{1, \ldots, n-1\}$, computes $a^{n-1} \mod n$ and outputs *n is composite*, if the result is not congruent to 1. Otherwise, the test outputs *n is probably prime*. Show that the test is correct. However, there are composite numbers n which are identified as possible primes for all $a \in \mathbb{Z}_n^*$. They are called *Carmichael* numbers. Show that $n = 561$ is a Carmichael number.
8. Check the primality of $n = 263$ with the Miller-Rabin algorithm. Use $a = 3$ and $a = 5$.
9. Encrypt $m = 2314$ with the plain RSA cipher and the public key ($e = 5$, $N = 10573$). Factorize N using Fermat's method. Why is $e = 5$ an admissible exponent, whereas $e = 3$ is not permitted? Determine the corresponding private key d. Decrypt the ciphertext and check the result. Use the Chinese Remainder Theorem to reduce the size of the exponents.
10. Two RSA moduli are given: $N_1 = 101400931$ and $N_2 = 110107021$. They have a common prime factor. Show that both RSA keys are insecure and compute the factorization of N_1 and N_2.
11. An adversary is able to modify a plain RSA ciphertext. He wants to square the corresponding unknown plaintext modulo N. Explain how to change the ciphetext. Why is this attack not possible for RSA-OAEP ?
12. Let $(e = 5, N = 10057)$ be the public key of an RSA cryptosystem. Encrypt the message $m = 2090$ using the plain RSA scheme. Factorize N and find the decryption exponent d.
13. Assume that RSA with a modulus of length 1024 bits and the encryption exponent $e = 2^{16} + 1$ is used. How many modular multiplications are needed, at most, for encryption and for decryption?
14. Factorize $N = 2041$ using the quadratic sieve method.
15. Factorize $N = 10573$ with Pollard's $p - 1$ method. Choose $a = 2$ and try $k = 2^3 3^3$, then give reasons why this attack is successful for the given integer N.

Supplement. The *Fast Exponentiation Algorithm* can be slightly optimized with the *Square-and-Multiply* algorithm.

Square-and-Multiply Algorithm

Input: Base $x \in \mathbb{N}$ and exponent $a = \sum_{i=0}^{s} h_i 2^i$ with $h_i \in \{0, 1\}$ and $a \geq 2$.
Output: $x^a \mod n$
Initialisation: $r = x$

```
for i = s − 1 downto 0 do
    r = r^2 mod n
    if h_i = 1 then
        r = r · x mod n
    end if
end for
return r
```

Example: $6^{41} = ((((6^2)^2 \cdot 6)^2)^2)^2 \cdot 6$. The computation is a sequence of squarings (SQ) and multiplications (MULT): SQ, SQ, MULT, SQ, SQ, SQ, MULT. As with the fast exponentiation algorithm, we need 5 quadratures and 2 multiplications, but in a different order. The exact order depends on the binary representation of the exponent. An advantage of this algorithm is that intermediate results do not need to be stored.

Key Establishment

Exercises

1. Show that the discrete-logarithm problem is easy in the *additive group* $(\mathbb{Z}_p, +)$.
2. How can you efficiently generate Diffie-Hellman parameters p, q and g for the multiplicative group $\mathbb{Z}_p^*$ with given bit lengths n_p and n_q for p and q ?
3. Let $p = 89$, $g = 2 \mod 89$ and $G = < g >$. How many different shared keys k are possible in a Diffie-Hellman key exchange with these parameters?
4. You perform a Diffie-Hellman key exchange with Alice and you agreed on the parameters $p = 43$, $G = < g > \subset GF(p)^*$ with $g = 3 \mod 43$.
   (a) Determine $q = \text{ord}\,(g)$.
   (b) Alice sends you $A = 14$ and you choose the secret exponent $b = 26$. Which value do you send to Alice? Compute the shared secret key k.
5. Let $g \equiv 3$ be an element of the group $\mathbb{Z}_{107}^*$.
   (a) Show that g generates a group G of prime order.
   (b) How many exponentiations at most are necessary to compute a discrete logarithm in G using the Babystep-Giantstep algorithm?
   (c) Compute $\log_3(12)$ in G.
6. Show that the following parameters (a 2048-bit MODP group given in RFC 5114) can be used in a Diffie-Hellman key exchange, i.e., show that p and q are prime numbers and $\text{ord}\,(g) = q$.
   Tip: Use SageMath. Remove the line breaks and define strings. The corresponding hexadecimal numbers can be constructed with `ZZ( ..., 16)`. Use the function `is_pseudoprime( )` to check the primality.

```
p = 87A8E61D B4B6663C FFBBD19C 65195999 8CEEF608 660DD0F2
    5D2CEED4 435E3B00 E00DF8F1 D61957D4 FAF7DF45 61B2AA30
    16C3D911 34096FAA 3BF4296D 830E9A7C 209E0C64 97517ABD
    5A8A9D30 6BCF67ED 91F9E672 5B4758C0 22E0B1EF 4275BF7B
    6C5BFC11 D45F9088 B941F54E B1E59BB8 BC39A0BF 12307F5C
    4FDB70C5 81B23F76 B63ACAE1 CAA6B790 2D525267 35488A0E
    F13C6D9A 51BFA4AB 3AD83477 96524D8E F6A167B5 A41825D9
    67E144E5 14056425 1CCACB83 E6B486F6 B3CA3F79 71506026
    C0B857F6 89962856 DED4010A BD0BE621 C3A3960A 54E710C3
    75F26375 D7014103 A4B54330 C198AF12 6116D227 6E11715F
    693877FA D7EF09CA DB094AE9 1E1A1597
```

```
g = 3FB32C9B 73134D0B 2E775066 60EDBD48 4CA7B18F 21EF2054
    07F4793A 1A0BA125 10DBC150 77BE463F FF4FED4A AC0BB555
    BE3A6C1B 0C6B47B1 BC3773BF 7E8C6F62 901228F8 C28CBB18
    A55AE313 41000A65 0196F931 C77A57F2 DDF463E5 E9EC144B
    777DE62A AAB8A862 8AC376D2 82D6ED38 64E67982 428EBC83
    1D14348F 6F2F9193 B5045AF2 767164E1 DFC967C1 FB3F2E55
    A4BD1BFF E83B9C80 D052B985 D182EA0A DB2A3B73 13D3FE14
    C8484B1E 052588B9 B7D2BBD2 DF016199 ECD06E15 57CD0915
    B3353BBB 64E0EC37 7FD02837 0DF92B52 C7891428 CDC67EB6
    184B523D 1DB246C3 2F630784 90F00EF8 D647D148 D4795451
    5E2327CF EF98C582 664B4C0F 6CC41659
q = 8CF83642 A709A097 B4479976 40129DA2 99B1A47D 1EB3750B
    A308B0FE 64F5FBD3
```

7. Why is RSA key encapsulation not CPA-secure without the hashing operation?
8. Discuss the consequences of re-using one or both of the secret Diffie-Hellman keys a and b.
9. Explain a *Man-in-the-Middle* attack against the Diffie-Hellman protocol.
10. The *ElGamal public-key encryption scheme* uses the same parameters as the Diffie-Hellman key-exchange, i.e., a cyclic group G, a generator g and $q = \text{ord}(g)$. For key generation choose a uniform number $a \in \mathbb{Z}_q$ and set $A = g^a \in G$. The message space is G, the ciphertext space is $G \times G$, the public key is $pk = (G, q, g, A)$ and the private key is $sk = (G, q, g, a)$. Encryption is randomized; to encrypt $m \in G$, one chooses a uniform random number $b \in \mathbb{Z}_q$ and defines the ciphertext as
$$\mathcal{E}_{pk}(m) = (g^b, A^b m).$$
Decryption is given by
$$\mathcal{D}_{sk}(c_1, c_2) = c_1^{-a} c_2.$$
    (a) Show that the scheme provides correct decryption.
    (b) Assume that $p = 59$, $G = GF(p)^*$, $g = 4$ and $a = 20$ define Alice's ElGamal key. She obtains the ciphertext $c = (17, 16)$. Compute the plaintext m.
    (c) The ElGamal encryption is randomized by a parameter b. Explain why b has to remain secret and should not be re-used for different encryptions.

Digital Signatures

Exercises

1. Give possible reasons why a signature can be invalid.
2. Suppose a new signature scheme takes pairs (m_1, m_2) of messages of the same length as input and defines a signature as follows: let $m = m_1 \oplus m_2$ and define $s = sign_{sk}(m)$ using a secure signature scheme. Is the new scheme secure or would you rather change this scheme?
3. Let $e = 5$, $N = 437$ be the parameters of a public RSA key. Verify the following plain RSA signatures:
   (a) $m = 102$, $s = 416$
   (b) $m = 101$, $s = 416$
   (c) $m = 100$, $s = 86$
   Conduct an existential forgery attack using the signature value $s = 99$.
4. Compute the RSA-FDH signature of a message m with hash value $H(m) = 11111$ using the RSA parameters $N = 28829$ and $e = 5$, where d has to be determined. Verify the signature with the public RSA key. *Hint:* $s = 7003$.
5. Consider the verification of a RSA-FDH signature. It is sufficient to give only the hash and the signature value to a verifier and not the message?
6. Why does the existential forgery attack almost certainly fail for RSA-PSS?
7. Discuss the consequences of a fixed and known salt value in RSA-PSS.
8. Show that the plain RSA signature scheme is secure under the RSA assumption if one considers the following experiment: the adversary succeeds if he outputs a valid signature of a challenge message, which is chosen uniformly at random and then given to the adversary.
9. Consider the Schnorr Identification Scheme. What happens if the parameter k is disclosed to an adversary? Does k have to be uniform random?
10. Suppose the Schnorr Identification Scheme is used with the multiplicative group $GF(p)^*$, $p = 59$, $g = 4 \mod 59$ and $q = 29$. Alice (the prover) chooses $x = 11$. Which is her public key and which is her private key? Alice then chooses $k = 7$. Bob (the verifier) sends her the challenge $r = 21$. Give Alice's initial message I and her response s. Show how Bob verifies her response.

11. The *ElGamal signature scheme* is based on the discrete logarithm problem and uses a cyclic subgroup G of $GF(p)^*$ of order q and a generator $g \in G$. One chooses a secret uniform $a \in \mathbb{Z}_q$ and computes $A = g^a$. Then $pk = (p, g, q, A)$ forms the public key and $sk = (p, g, q, a)$ the private key. The signature generation is randomized; one chooses a random uniform $k \in \mathbb{Z}_q^*$ and computes the signature value

    $$sign_{sk}(m) = (r, s) \text{ with } r \equiv g^k \mod p \text{ and } s \equiv k^{-1}(H(m) - ar) \mod q.$$

    To verify the signature (r, s) of a message m, one computes $A^r\, r^s \mod p$ and compares the result with $g^{H(m)} \mod p$. If both residue classes coincide, the signature is valid.
    (a) Show that the verification is correct.
    (b) Assume that $p = 59$, $g = 4 \mod 59$, $q = 29$ and $a = 20$ form Alice's ElGamal key. Compute the public key A.
    (c) Alice wants to sign a message m with hash value $H(m) = 8$. She chooses the secret parameter $k = 5$. Compute the ElGamal signature (r, s).
    (d) Check that the signature (r, s) is valid.
    (e) The ElGamal signature is randomized with the parameter k. Explain why k must remain secret and should not be re-used for different signatures.

12. Consider the *Digital Signature Algorithm (DSA)* with the multiplicative group $GF(p)^*$.
    (a) Assume that Alice's key is given by $p = 59$, $g = 4 \mod 59$, $q = 29$ and $x = 20$. Compute the public key y.
    (b) Alice wants to sign a message m with hash value $H(m) = 8$. She chooses the secret parameter $k = 5$. Compute the DSA signature (r, s).
    (c) Check that the signature (r, s) is valid.
    (d) The DSA signature is randomized with the parameter k. Explain why k must remain secret and must not be re-used for different signatures.

Elliptic Curve Cryptography

Exercises

1. Let $K = GF(3)$ and let E be the elliptic curve defined by $y^2 = x^3 + x + 2$ over K.
   (a) Enumerate all elements of the affine space K^2 and the projective space $\mathbb{P}^2(K)$.
   (b) Give the equation of the projective elliptic curve.
   (c) Why is the Weierstrass equation nonsingular?
   (d) Enumerate all points in $E(K)$.
   (e) $P = (1, 1)$ and $Q = (2, 0)$ are points in $E(K)$. Draw a line through P and Q and find the point R such that $P + Q + R = O$. Then give $P + Q$.
   (f) Use the preceding parts to show that ord $(P) = 4$. Then determine the group structure of $E(K)$.

2. Let E be the elliptic curve defined by $y^2 = x^3 + 3x + 5$.
   (a) Assume that E is defined over $K = GF(19)$. Compute the discriminant Δ. Show that $P = (4, 9) \in E(GF(19))$ and compute $2P$.
   (b) Compute $13P$.
   (c) Give points of order 1, 2, 13 and 26 in $E(GF(19))$.
   Hint: ord $(E(GF(19))) = 26$. Now use the preceding parts.
   (d) Now let E be defined over $K = \mathbb{Q}$. Compute the discriminant Δ. Show that $P = (4, 9) \in E(\mathbb{Q})$ and compute $2P$.

3. Suppose E is an elliptic curve over $K = GF(23)$.
   (a) Give the minimum and the maximum number of points on $E(K)$.
   (b) How many point additions or doublings are at most needed to compute nP for any $n \in \mathbb{Z}$ and $P \in E(K)$?

4. We consider the domain parameters of the curve `brainpoolP256r1` (RFC 5639). The curve is defined by the Weierstrass equation $y^2 = x^3 + a_1x + b_1$ over a 256-bit field $K = GF(p)$. The base point $g = (x_g, y_g)$ generates the full group $G = E(K)$ and $n = \text{ord}\,(g)$ is a 256-bit prime number.

```
p =  A9FB57DBA1EEA9BC3E660A909D838D726E3BF623D52620282013481D1F6E5377
a1 =  7D5A0975FC2C3057EEF67530417AFFE7FB8055C126DC5C6CE94A4B44F330B5D9
b1 =  26DC5C6CE94A4B44F330B5D9BBD77CBF958416295CF7E1CE6BCCDC18FF8C07B6
g =  (xg,yg)
```

```
xg=  8BD2AEB9CB7E57CB2C4B482FFC81B7AFB9DE27E1E3BD23C23A4453BD9ACE3262
yg=  547EF835C3DAC4FD97F8461A14611DC9C27745132DED8E545C1D54C72F046997
n  = A9FB57DBA1EEA9BC3E660A909D838D718C397AA3B561A6F7901E0E82974856A7
h  = 1
```

Show that these parameters are valid, i.e., that p and n are prime, $\Delta \neq 0 \mod p$ and $\text{ord}\,(g) = n$.
Hint: Use SageMath. Hexadecimal numbers can be defined using the prefix `0x`. Check the primality using `is_prime()`. Define the elliptic curve `E=EllipticCurve(GF(p),[a,b])` and the point `g=E(xg,yg)`. The order of $E(K)$ can be obtained by `E.order()`.

5. Use the domain parameters of the above Exercise 4 for an Elliptic Curve Diffie-Hellman key exchange. Assume that Alice and Bob choose the following secret parameters:

   ```
   a=81DB1EE100150FF2EA338D708271BE38300CB54241D79950F77B063039804F1D
   b=55E40BC41E37E3E2AD25C3C6654511FFA8474A91A0032087593852D3E7D76BD3
   ```

   Compute A, B, bA, aB and k.

6. The shared secret of an Elliptic Curve Diffie-Hellman key exchange is a point on an elliptic curve. Why is only the x-coordinate used in a subsequent key derivation?

7. Consider the *Elliptic Curve Digital Signature Algorithm* (ECDSA).
   (a) Show that signature verification is correct.
   (b) Use the elliptic curve in Exercise 2 over $K = GF(19)$ with base point $g = (18, 18)$ and $n = \text{ord}\,(g) = 13$. Alice's secret key is $a = 2$. She wants to sign a message m with $H(m) \equiv 11 \mod n$ and chooses $k = 3$. Compute the signature (r, s) and verify the signature using her public key.
   (c) Show that k must remain secret.