7. Exam preparation sheet

You will find the following remarks on the exam:

- Verify whether your exam exercise sheets are complete: It should contain Exercise 1 to Exercise 7. Insert your name and matrikel (student number) on each sheet. Approaches, solutions and all side calculations must be written to the given paper. Please use also the back sides. If you need extra paper ask the supervisor. **Do not remove the staple!**

- **Do write with blue or black ink!**
- **Do not use a pencil or any other erasable pen.**

The exam must be handled independently. Permitted auxiliary means are: writing materials, a pocket calculator (non-programmable, without division with remainder, without linear algebra software), and a cheat sheet, DIN A4, two-sided, written only with your own handwriting. Any other utilities, even own paper, are not permitted.

**An attempt at deception leads to failure for this exam and possibly other measures — even if the attempt is only detected later.**

---

**Exercise 1** (Democratic elections). (0 points)

What are the main properties of democratic elections? Sketch them and their interrelations. (In particular: Which properties do we need for free elections, which for fair elections?)

---

**Exercise 2** (Tool: The Extended Euclidean Algorithm). (0 points)

(i) Find \( s, t \in \mathbb{Z} \) such that \( s \cdot 17 + t \cdot 39 = 1 \).

(ii) Find \( s, t \in \mathbb{Z} \) such that \( s \cdot 14 + t \cdot 55 = 1 \).

(iii) Find \( s, t \in \mathbb{F}_2[x] \) such that \( s \cdot (x + x^3 + x^5) + t \cdot (1 + x + x^3 + x^4 + x^8) = 1 \).

---

**Exercise 3** (RSA). (0 points)

Let’s ‘play’ at RSA. Use the primes \( p = 71 \), \( q = 79 \) and \( e = 17 \).

(i) Compute secret and public key.

(ii) Explain how to encrypt \( x = 991 \).

(iii) Explain how to decrypt \( y = 99 \).

(iv) Explain why encrypting \( x \) giving \( y \) and then decrypting the \( y \) giving \( z \), always gives \( z = x \). Go back to the theorem of Lagrange, Euler or Fermat. (Cite the theorem that you use.)
Exercise 4 (Blind signatures).

The following questions describe a blinding protocol based on the RSA signature scheme. Let B have the RSA public key $(N, e)$ and secret key $(N, d)$. In order to receive blind signatures from B, party A uses an own blinding key $b \in \mathbb{Z}_N^\times$:

**Protocol.** Blind signature.

**Input:** Party A has a message $x \in \mathbb{Z}_N^\times$.

**Output:** Party A gets a signature $S(x)$ such that $S(x)^e = x$ in $\mathbb{Z}_N^\times$ where $(N, e)$ is B’s public key.

1. A chooses $b \leftarrow \mathbb{Z}_N^\times$ and sends $X = x \cdot b^e \in \mathbb{Z}_N^\times$ to B.
2. B produces the signature $S(X) = X^d \in \mathbb{Z}_N^\times$ and sends it to A.
3. A recovers $S(x) = b^{-1} \cdot S(X) \in \mathbb{Z}_N^\times$.

(i) Let $N = p \cdot q$ where $p = 1000000000037, q = 100000100021$ and $e = 2^{16} + 1 = 65537$. Compute the secret exponent $d$ of B. Let $k \in \mathbb{Z}_N^\times$ be a random number and $m \in \mathbb{Z}_N^\times$ be the integer value of the ASCII text: `blinded`.

(a) Compute the blinded message $M$.

(b) Compute B’s blinded signature $S(M)$ and also B’s clear text signature $S'(m)$, using B’s secret key $d$.

(c) Compute the clear text signature $S(m)$ such as A recovers it using $k$. Compare this signature to the value $S'(m)$ above.

Exercise 5 (ElGamal signatures).

We choose a prime number $p = 12347, q = 6173$, and the group $G = \langle g \rangle < \mathbb{Z}_p^\times$ with $g = 2^2$. We use $\alpha = 5432$ as the secret part of the key $K = (p, q, g, \alpha, a)$. The function $\star: \langle g \rangle \rightarrow \mathbb{Z}_q$ is defined by $\star(k \mod p) = k \mod q$ for $0 < k < p$. The hash function is essentially the identity: hash$(x) = x \mod q$. The message $x$ to be signed consists of the least significant four digits of your student registration number. Use $\beta = 399$ as your random number from $\mathbb{Z}_p^{\times}$. Example: If the student registration number is 1234567, then $x = 4567$.

(i) Show: the order of $g$ and the size of $G$ is $q$.

or better: show that $h = 2$ generates $\mathbb{Z}_p^\times$ and conclude the prior from it. (Ie. $\# \langle h \rangle = p - 1$.)

(ii) Compute the public key $a = g^\alpha \in G$.

(iii) Compute the signature $\text{sig}_K(x, \beta) = (x, b, \gamma)$.

(iv) Verify your signature.
Exercise 6 (Security of a re-encryption mixnet). (0 points)

We want to prove that the security of a re-encryption mixnet based on ElGamal can be reduced to the security of the underlying ElGamal encryption scheme. In other words: if we can break the anonymity of the mixnet then we can also break ElGamal encryption.

In the entire exercise we only consider a key-only attack, ie. the attacker only gets the setup.

Note that the security of the ElGamal encryption scheme is equivalent to the so-called decisional Diffie-Hellman problem for the underlying group $G$, which is given four elements $g, g^\alpha, g^\beta, g^\gamma \in G$ decide whether $\alpha \beta = \gamma$ (?).

We work in some (multiplicatively written) group $G$ generated by an element $g$ of order $q$, all this specified in the global setup. The receiver of the mixnet has the private key $\alpha \in \mathbb{Z}_q$ which defines the public key $a = g^\alpha \in G$. We use $\text{enc}_a(x, \varrho) = (g^\varrho, a^\varrho x)$ and $\text{dec}_\alpha(r, y) = y r^{-\alpha}$.

(i) Check that $\text{dec}_\alpha(\text{enc}_a(x, \varrho)) = x$.

- The attacker $A$ is given input and output of one particular mix, ie. a list of encrypted messages $(g^{e_i}, a^{e_i} x_i)_{i \in I}$ and a re-encrypted and re-order list $(g^{e_i}, a^{e_i} x_{\sigma(i)})_{i \in I}$ where $\sigma$ is a permutation of $I$. The random exponents $\varrho_i, g'_i$ and the permutation $\sigma$ are unknown to the attacker.
- The attacker tries to determine $\sigma^{-1}(i_0)$ for some element $i_0 \in I$.
- Suppose that he can always do so.
- The reducer, that is you, is given four elements $(g, a, g^\varrho, b)$ and tries to determine whether $b = a^\varrho$. The reducer is allowed to query the attacker and prepare the attacker’s entire environment, ie. all its inputs, also those coming from oracles.
- You feed the attacker with
  - the mix’s input $c_0 = (g^\varrho, bx), c_1 = (g^{e_1}, a^{e_1} x)$, and
  - the mix’s output $c'_0 = (g^{k_0} g^\varrho, a^{k_0} bx), c'_1 = (g^{e'_1}, a^{e'_1} x)$.

(ii) Argue that we can execute all operations in polynomial time. (Where a call to the attacker only counts as a single time unit.)

(iii) Prove that the ciphertext $c'_i$ is a re-encryption of ciphertext $c_i$. In other words, $c_0$ and $c'_0$ are both encryptions of $bx$, and $c_1$ and $c'_1$ are both encryptions of $x$.

(iv) Decrypting $c_0$ we get $\text{dec}_\alpha(c_0) = b x a^{-\varrho}$. Prove that this is equal to $x$ if and only if $b = a^\varrho$.

(v) Prove that if $b \neq a^\varrho$ the attacker will answer that $\sigma^{-1}(1) = 1$.

(vi) Prove that if $b = a^\varrho$ the attacker can only guess and will answer 0 or 1 at random. (Assume that the attacker chooses uniformly if there is an ambiguity.)
Now, you play the above game twice (say), and answer “$b \neq a^e$” if and only if the attacker answers $\sigma^{-1}(1) = 1$ in both queries.

(vii) Prove that you give the correct answer with probability at least 75%.

(viii*) Suppose that the attacker only succeeds with a considerable advantage over guessing, say $\text{prob}(\mathcal{A}(\ldots) = \sigma^{-1}(1) = 1^r) > \frac{3}{4}$. (Here, $n$ is the security parameter, say the length $q$ in bits, and $c$ is some constant depending on $\mathcal{A}$ only.) Prove that you still answer correctly with probability at least $\frac{9}{16}$.

Refining all this leads to the theorem:

**Theorem.** Assume that at least one mix of an ElGamal re-encryption mixnet is uncorrupted.

If the decisional Diffie-Hellman problem is intractable, then the mixnet is (computationally) anonymous.

If ElGamal encryption is secure against a key-only attacker trying to distinguish the encryptions of (one of) two self-chosen plaintexts, then the mixnet is (computationally) anonymous.

**Exercise 7** (An electronic voting scheme). (0 points)

The scheme by Chaum (1981) proceeds in three stages.

**Registration** Each voter submits a temporary (one-time) public encryption key through a decryption mixnet to a bulletin board.

**Voting** The voter encrypts his vote with the temporary private encryption key and submits it together with the temporary public encryption key through a decryption mixnet to another bulletin board.

**Tallying** All votes are open on the bulletin board: so just inspect that!

(i) Explain why the voting is anonymous.

(ii) Explain why the voter does not have a receipt.

(iii) How is eligibility granted?

(iv) Which problems remain to be solved?