Cryptography and Security — Final Exam

Serge Vaudenay

29.1.2026

- duration: 3h00
- no documents allowed, except one 2-sided sheet of handwritten notes
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will **not** answer any technical question during the exam
- readability and style of writing will be part of the grade
- answers should not be written with a pencil

1 Mersenne Cryptosystem

A Mersenne number is an integer of the form $p = 2^n - 1$. When it is prime, it is called a Mersenne prime. There exists a few known large Mersenne primes such as $p = 2^{756\,839} - 1$.

In this exercise, we fix n such that $p = 2^n - 1$ is prime. Given an integer x, we denote by $\mathsf{HW}(x)$ the Hamming weight of the binary representation of $x \bmod p$ (i.e. the number of bits which are equal to 1 once x has been reduced modulo p).

Q.1 For any list $(s_1, \ldots, s_k)$ of non-negative integers (not necessarily bounded by n), prove that $\mathsf{HW}(2^{s_1} + \cdots + 2^{s_k}) \leq k$.

Q.2 For any integer A and B, prove that $\mathsf{HW}(A + B) \leq \mathsf{HW}(A) + \mathsf{HW}(B)$ and $\mathsf{HW}(AB) \leq \mathsf{HW}(A) \times \mathsf{HW}(B)$.

Q.3 For $X \in \mathbf{Z}_p$ uniformly distributed and a constant integer s, give the distribution of $\mathsf{HW}(X \oplus Y)$ where $Y = (X + 2^s) \bmod p$. (Here, $\oplus$ is the bitwise exclusive or of the modulo p binary representation.) Namely, prove that $\Pr[\mathsf{HW}(X \oplus Y) = i] = \frac{2^{n-i}}{p}$ for $i = 1, \ldots, n$.

HINT: reduce to the $s = 0$ case.

Q.4 For $X \in \mathbf{Z}_p$ uniformly distributed and a constant δ such that $\mathsf{HW}(\delta) = k$, we let $Y = (X + \delta) \bmod p$. Prove that $\Pr[\mathsf{HW}(X \oplus Y) \geq i] \leq k 2^{2-\frac{i}{k}}$.

HINT: set $\delta = \sum_{i=1}^{k} 2^{s_i}$, $X_0 = X$, and $X_i = (X_{i-1} + 2^{s_i}) \bmod p$.

Q.5 Given a security parameter λ, we define some parameters h, n, p such that $h = \lambda$, $10h^2 \leq n \leq 16h^2$, $p = 2^n - 1$, and p prime. Using these parameters, a key generation algorithm $\mathsf{Gen}(h, n, p)$ first picks at random $F, G, R \in \mathbf{Z}_p$ such that $\mathsf{HW}(F) = \mathsf{HW}(G) = h$. Then, it sets $T = (FR + G) \bmod p$, $\mathsf{pk} = (R, T)$, and $\mathsf{sk} = F$. The output is pk and sk. Moving ahead, we define a cryptosystem with Gen as a key pair generator. We consider the problem of winning in the following game (where the winning condition is missing):

Input: h, p

1: pick $(F, G, R) \in \mathbf{Z}_p^3$ satisfying $\mathsf{HW}(F) = \mathsf{HW}(G) = h$ uniformly
2: $T \leftarrow (FR + G) \bmod p$
3: $F' \leftarrow \mathcal{A}(h, p, R, T)$
4: **return** 1_{win}

Write down the game defining security against key recovery under chosen plaintext attacks and define the winning condition in the above game so that the two games become equivalent.

Q.6 We assume an efficient encoding algorithm $\mathcal{E}$ mapping a message m in a message domain to $\mathcal{E}(m) \in \mathbf{Z}_p$ and an efficient decoding algorithm $\mathcal{D}$ such that $\mathcal{D}(\mathcal{E}(m) \oplus e) = m$ for any message m and any $e \in \mathbf{Z}_p$ satisfying $\mathsf{HW}(e) \leq \tau$, for a given threshold τ. We define the encryption of m as follows: we pick A, B_1, B_2 in $\mathbf{Z}_p$ satisfying $\mathsf{HW}(A) = \mathsf{HW}(B_1) = \mathsf{HW}(B_2) = h$ uniformly, then $C_1 = (AR + B_1) \bmod p$ and $C_2 = ((AT + B_2) \bmod p) \oplus \mathcal{E}(m)$, and output $\mathsf{ct} = (C_1, C_2)$. The decryption of ct is $m' = \mathcal{D}(((FC_1) \bmod p) \oplus C_2)$. Prove that the cryptosystem is correct but for some probability up to ε to upper bound based on h, p, and τ.

2 Nonce Repetition in ML-DSA

We recall the ML-DSA signature algorithm as seen in class. We use

$$q = 8\,380\,417 = 2^{13} \times 3 \times 11 \times 31 + 1$$

$R_q = \mathbf{Z}_q[X]/(X^{256} + 1)$, and some parameters k and ℓ (say for example $k = \ell = 4$). We use a hash function H with range in the set of small elements of R_q. We also define a function round from $\mathbf{Z}_q$ to $\mathbf{Z}_q$ (that we extend to a function from R_q^i to R_q^i by applying to each coefficient) which rounds a modulo-q residue to the nearest one which is ending by ℓ zero bits.

- To generate a key pair, we pick $A \in R_q^{k \times \ell}$ uniformly and $s_1 \in R_q^\ell$ small. We set $t_1 = \mathsf{round}(As_1)$. Finally, $\mathsf{sk} = s_1$ and $\mathsf{pk} = (A, t_1)$.
- To sign a message M, we compute $\mu = H(0\|M)$, we pick a nonce $y \in R_q^\ell$ small, we set $w = \mathsf{round}(Ay)$, $c = H(\mu, w)$, $z = y + cs_1$, and the signature is $\sigma = (c, z)$.
- To verify a signature σ for M, we check that z is small. We compute μ and $w_\approx = Az - ct_1$. We check that $c = H(\mu, \mathsf{round}(w_\approx))$.

Q.1 Given two different signed messages which are using the same nonce, show how to do a key recovery attack.

Q.2 Given a collection of n signed messages in which two are using the same nonce, give an algorithm to identify those two signed messages and analyze the complexity.

Q.3 What is the improvement about nonce-misuse issues compared to DSA or ECDSA?

3 Machine-Readable Travel Documents

We recall the principle of machine-readable travel documents (MRTD). If a holder shows the opened MRTD to a reader, the reader can optically read a machine-readable zone (MRZ). It contains some information which is used as a password. It consists of: a serial number (8 upper-case alphanumerical characters), a date of birth, an expiration date. Given this information, the reader and the NFC chip can run a password authenticated key exchange (PAKE) and open a secure communication channel. Then, the chip provides the reader with the mandatory elements: a digital copy of the MRZ (called DG1), a picture to be used as a model for facial recognition (called DG2), an element SOD. The SOD includes the list of the hash of each DGi which is present in the chip and requires passive authentication, the signature of this list by the issuer, and the certificate of the issuer. The MRZ contains other information such as the name of the holder, their nationality and their gender.

Q.1 What is the difference between the digital image in DG2 and a regular digital picture?
Q.2 Compared to traditional travel documents, explain what the SOD leaks.
Q.3 Estimate the entropy (in bits) of the password.
Q.4 Compare the security of the password with the one of a regular password chosen by a human user. What is the risk of a disclosed MRTD password?