

Exercise Sheet 5

Cryptography and Security 2025

Exercise 1 RSA with a counter

In this exercise, we consider the plain RSA protocol, i.e.

Setup Let $N = pq$ and $\varphi(N) = (p-1)(q-1)$ where p, q are two random $\frac{\ell}{2}$ -bit primes. Pick a random e such that $\gcd(e, \varphi(N)) = 1$ and let $d = e^{-1} \bmod \varphi(N)$. The public key is $K_p = (e, N)$ and the private key is $K_s = (d, N)$.

Encryption On input message $m \in \{0, \dots, N-1\}$, the ciphertext is $c = m^e \bmod N$.

Decryption On input ciphertext c , the message is recovered computing $m = c^d \bmod N$.

We assume a protocol in which every messages are RSA-encrypted with exponent $e = 3$. To protect the sequentiality of protocol messages, messages are concatenated with a 32-bit counter before encryption. Hence, if Alice wants to send a i^{th} message equal to m to Bob, she sends $(\text{format}(m) \cdot 2^{32} + i)^e \bmod N_B$ where N_B is Bob's RSA modulus and $\text{format}(m)$ is a formatted string consisting of m concatenated with an integrity check $H(m)$. Upon reception, Bob decrypts, checks that the index number i is as expected, checks the redundancy in the formatted string, and finally extracts m . Messages from Bob to Alice use another counter and Alice's RSA modulus N_A .

1. Which security property is protected by this protocol? Which security property is not? (Confidentiality? Authentication? Integrity?) Explain why.
2. After Alice sends some $a = x^e \bmod N_B$ to Bob, an adversary impersonates the response "could you repeat please" from Bob to Alice. Alice repeats the same message by sending some $b = y^e \bmod N_B$.
 - (a) What is the relation between x and y ?
 - (b) In the ring $\mathbb{Z}_{N_B}[z]$ of polynomials with unknown z and coefficients in \mathbb{Z}_{N_B} , show that $z - x$ is a factor of $z^3 - a$ and $(z + 1)^3 - b$.
 - (c) Deduce that $z - x$ is the gcd of $z^3 - a$ and $(z + 1)^3 - b$ in this ring.
 - (d) From the previous question, apply the Euclid algorithm to find a rational expression for x in terms of a and b .
3. Can this extend to $e = 65537$?

Exercise 2 Quadratic Residues

Let $n = p_1 \times p_2 \times \dots \times p_k$ where p_1, \dots, p_k are distinct odd primes and an integer $k \geq 2$. The element $a \in \mathbf{Z}_n^*$ is said to be a *quadratic residue* (QR) modulo n if there exists an $x \in \mathbf{Z}_n^*$ such that $x^2 \equiv a \pmod{n}$. If no such x exists, then a is called a *quadratic non-residue* (QNR) modulo n . Note that the non-invertible elements of \mathbf{Z}_n are neither quadratic residues nor quadratic non-residues.

1. Find the QR's and QNR's of \mathbf{Z}_{35}^* . How many square roots does each of these QR's possess?

2. We call “CRT-transform”, the ring isomorphism used in the Chinese Remainder Theorem. Prove that an element $a \in \mathbf{Z}_n^*$ is a QR modulo n if and only if each component of its image under the “CRT-transform” with respect to the moduli p_1, \dots, p_k is a QR of $\mathbf{Z}_{p_i}^*$.
3. Show that a QR of \mathbf{Z}_n^* has exactly 2^k distinct square roots in \mathbf{Z}_n^* .
4. Show that the QR's of \mathbf{Z}_n^* form a subgroup of \mathbf{Z}_n^* . What is the order of this subgroup?
5. Show that the product of a QR of \mathbf{Z}_n^* and a QNR of \mathbf{Z}_n^* is always a QNR of \mathbf{Z}_n^* .
6. Exhibit some examples in \mathbf{Z}_{35}^* which show that the product of two QNR's of \mathbf{Z}_{35}^* can be either a QR or a QNR of \mathbf{Z}_{35}^* .

Exercise 3 Modulo 101 Computation

Through *all* this exercise, we will let $p = 101$.

1. Show that p is a prime number.
2. What is the order of \mathbf{Z}_p^* ?
3. If $x = \sum_{i=0}^{2\ell-1} d_i 10^i$ with $0 \leq d_i < 10$ for all i , show that

$$x \equiv \sum_{i=0}^{\ell-1} (-1)^i (d_{2i} + 10d_{2i+1}) \pmod{101}$$

Deduce an algorithm to compute $x \pmod{101}$ easily.

4. Show that every element of \mathbf{Z}_p^* has a unique 7th root and give an explicit formula to compute it (recall that $p = 101$).
Application: Find the 7th root of 2 in \mathbf{Z}_p^* .
5. Given $g \in \mathbf{Z}_p^*$ we let $y = g^{10} \pmod{p}$. Using 3 multiplications modulo p and 2 tests, give an algorithm with input y to decide whether g is a generator or not (recall that $p = 101$).
Application: show that 2 is a generator.
6. Under which condition is x a quadratic residue in \mathbf{Z}_p^* ?
7. Show that 5 is a quadratic residue in \mathbf{Z}_p^* .
8. Show that 10 is a 4th root of 1 in \mathbf{Z}_p^* .
9. Show that for all $y \in \mathbf{Z}_p^*$ we have that $y^{\frac{p-1}{4}}$ is 10^k for some $k \in \{0, 1, 2, 3\}$.
 Show that $y^{\frac{p+3}{4}}$ can be written $y \times 10^k$.
10. Deduce that if x is a quadratic residue then either $x^{\frac{p+3}{8}}$ or $10x^{\frac{p+3}{8}}$ is a square root of x . Provide an algorithm to extract square roots in \mathbf{Z}_p^* .
11. Find a square root of 5.