Introduction to cryptology
TD#6

2019-04

In the following exercises, $N = pq$ for distinct prime numbers p and q; $e, d \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^\times \backslash \{1\}$ such that $ed \equiv 1 \mod \varphi(N)$; RSA-P : $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ is defined by $m \mapsto m^e \mod N$, and its inverse RSA-P^{-1} is defined by $m \mapsto m^d \mod N$.

Exercise 1: Semi-homomorphic property of an RSA permutation

Q. 1: Let m, $m' \in \mathbb{Z}/N\mathbb{Z}$, $c = \text{RSA-P}(m)$, $c' = \text{RSA-P}(m')$. Give an expression for cc' of the form x^e (for some x). Use this expression to compute the value RSA-P$^{-1}(cc')$.

Q. 2: Explain how the above property allows to multiply two numbers without decrypting them.

Q. 3: Note that the above procedure is deterministic. Does a modified procedure that works with encrypted numbers of the form pad(x) (where pad is a non-deterministic function) still allow to multiply numbers in encrypted form?

Exercise 2: RSA-CRT

Q. 1: Let $C_p = q \times (q^{-1} \mod p)$; $C_q = p \times (p^{-1} \mod q)$.

1. Compute the following: $C_p \mod p$; $C_p \mod q$; $C_q \mod p$; $C_q \mod q$.

Q. 2: Let $0 \leq x < N$ be such that $x \equiv x_p \mod p$; $x \equiv x_q \mod q$.

1. Using the Chinese Remainder Theorem (CRT), give the value of x in function of C_p, x_p, C_q, x_q and N.

Q. 3: A user wishes to implement RSA-P^{-1} by computing the exponentiation to d using the CRT.

1. Explain why if RSA-P and RSA-P^{-1} are used within an RSA cryptosystem, a CRT implementation may only be used by someone knowing the private key
2. Give the details of such an implementation.

Q. 4: We now want to show that if a *single fault* occurs during the CRT computation of $m^d \mod N$, the faulty result may be used to factor N. Let $u = m^d \mod N$ be the expected result of the computation and v be a faulty result such that $v \equiv u \mod p$, $v \not\equiv u \mod q$.

1. Give an expression for $a := u^e \mod N$ in function of m, C_p, C_q, p, q, and N.

2. Give an expression for $b := v^e \mod N$ in function of m, C_p, C_q, p, q, N, and an unknown quantity x.
3. Show that $\gcd((a - b), N)$ reveals a non-trivial factor of N.

Exercise 3: Domain of an RSA permutation

Q. 1: Using the extended Euclid algorithm, show that if $0 < \alpha < N$ is such that $\gcd(\alpha, N) = 1$, then α has a multiplicative inverse modulo N. Show then that for any $e > 0$, α^e is invertible modulo N.

Q. 2: Consider now $0 < \alpha < N$ with $\gcd(\alpha, N) = p$. What is the value of $\alpha \mod p$? Does α have an inverse modulo N? What is $\gcd(\alpha, q)$ equal to? Using the CRT, how many such elements are there in $\mathbb{Z}/N\mathbb{Z}$? What is $\alpha^{q-1} \mod q$ equal to?

Q. 3: Let $0 < u < N$ be the unique number modulo N that verifies $u = 0 \mod p$, $u = 1 \mod q$. How can you compute u using inversion modulo q? Let α be as in the above question; what are $\alpha^{q-1} \mod N$ and $\alpha^{k(q-1)} \mod N$ (for any k) equal to? Give a necessary condition on e for the map $x \mapsto x^e$ to be invertible on α.

Q. 4: Let $e \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^\times$, $d = e^{-1}$. What is $ed \mod (p-1)(q-1)$ equal to? What is $\alpha^{ed} \mod q$ equal to? And $\alpha^{ed} \mod N$? Are there any elements not invertible by $x \mapsto x^e$? What is the domain of an RSA permutation?