Cryptology complementary
Exercises #5

2018-W15

In the following exercises, we let $N = pq$ be the product of two prime numbers, $e \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^\times$, $d = e^{-1}$. We define the RSA permutation RSA-P with parameters N and e as RSA-P : $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, $m \mapsto m^e$. Its inverse is given by $c \mapsto c^d$.

Exercise 1: 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. Does this guarantee that $x \mapsto x^e$ is invertible over $(\mathbb{Z}/N\mathbb{Z})^\times$?

Q. 2: Consider now $0 < \alpha < N$ with $\gcd(\alpha, N) = p$. What is the value of $\alpha \mod p$ (meaning the remainder of the division of α by p, abusing notations)? Does α have an inverse modulo N? What is $\gcd(\alpha, q)$? How many such elements are there in $\mathbb{Z}/N\mathbb{Z}$? What is $\alpha^{q-1} \mod q$?
The goal of the next questions is to characterize the values of multiples of p modulo N.

Q. 3: Let $0 < u < N$ be the unique number that verifies $u \equiv 0 \mod p$, $u \equiv 1 \mod q$. Show how to compute u using the CRT (i.e. using inversion modulo q)?

Q. 4: Let again α be as in **Q. 2**. Using the result of **Q. 3**, find $0 < \beta < N$ s.t. $\alpha^{q-1} \equiv \beta \mod N$. Idem for $0 < \gamma < N$ s.t. $\alpha^{k(q-1)} \equiv \gamma \mod N$ (for any k)? Give two necessary conditions on e for the map $x \mapsto x^e$ (over $\mathbb{Z}/N\mathbb{Z}$) to be invertible.

Q. 5: Let $e \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^\times$, $d = e^{-1}$. Show that $\alpha^{ed} \equiv \alpha \mod q$; $\alpha^{ed} \equiv \alpha \mod N$. Are there any elements not invertible by $x \mapsto x^e$? What is the domain of an RSA permutation?

Exercise 2: 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 $\text{RSA-P}^{-1}(cc')$.

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?