Sécurité des systèmes d'information
Exercise sheet 4 : Asymmetric Cryptography

30 Octobre 2019

Non-mandatory exercise sheet. Please upload your answers on Moodle before Monday **4/11/2019 17h15**.

All answers should be carefully justified.

Exercise 1 : Math Warmups

- Let p be a prime number. Compute $\phi(p^k)$ by counting all numbers $a \leq p^k$ such that $\gcd(a, p^k) > 1$.
- Using the Chinese Remainder theorem, explain why $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ whenever $gcd(a, b) = 1$.
- By using the prime factorization of any number n, explain the general formula for $\phi(n)$ using preceding steps.

Exercice 1 : RSA

- Let p = 11, q = 17. Create a set of keys for RSA
- Let (n=247, e=17) be the public key. Use it to encode the message "28". Find then two prime numbers p,q and compute the encryption exponent d (use extended euclidean algorithm). Finally, decode the encoded message to check your computations.

Exercice 2 : Rabin

On recall Rabin cryptographic algorithm :

- *Keys generation* : A chooses two big prime numbers p and q, that he keeps secret. He chooses them such that $p \equiv q \equiv 3 \mod 4$ (to make decryption easier). A then computes $n = p \cdot q$.

- *Keys Distribution* : A sends n, his public key to B. (p and q are secrets and are never shared).
- *Encryption* : B encrypts his message m by calculating $c = m^2 \mod n$. B then sends his cipher c to A.
- *Decryption* : A computes $m = \sqrt{c} \mod n$ by following the steps :
  1. A computes $m_p = \sqrt{c} = c^{\frac{p+1}{4}} \mod p$ and m_q similarly (note how $p \equiv q \equiv 3 \mod 4$ simplifies this step).
  2. A solves the system of two equations
     $m = m_p \mod p$
     $m = m_q \mod q$
     he obtains four solutions among which he finds the original message m.

     Writing $p_1 = p^{-1} \mod q$ and $q_1 = q^{-1} \mod p$, we have

$$\begin{array}{rcl} m_1 & = & (m_p \cdot q \cdot q_1 + m_q \cdot p \cdot p_1) \mod n \\ m_2 & = & (m_p \cdot q \cdot q_1 - m_q \cdot p \cdot p_1) \mod n \\ m_3 & = & (-m_p \cdot q \cdot q_1 + m_q \cdot p \cdot p_1) \mod n \\ m_4 & = & (-m_p \cdot q \cdot q_1 - m_q \cdot p \cdot p_1) \mod n \end{array}$$

You are B, And you receive A's public key which is 253 :

- Compute the Cipher of the message 134.
- Find the prime factors p et q of n.
- Uncipher the message by computing m_p and m_q, then compute all 4 possible messages m_1, m_2, m_3 and m_4 (You should find 134 among these results).

Exercice 3 : ElGamal

We recall ElGamal Cipher :

- *Keys Generation* : Each entity generates his own couple of keys, a private and a public key.
  A generates a big prime number p, and a generator α from the multiplicative group $\mathbb{Z}_p^*$. A then generates a random number $a < p-1$, and computes $\alpha^a \mod p$.
  The public key of A is (p, α, $\alpha^a \mod p$), his private key is a.
- *Encryption* : B encrypts the message m ($m < p$) by generating a random number $k < p-1$. B computes $\lambda = \alpha^k \mod p$ and $\sigma = m \cdot (\alpha^a)^k \mod p$. Finally, B send his cipher c = (λ,σ) to A.

- *Decryption* : A computes $x = \lambda^{p-1-a} \equiv \lambda^{-a} \equiv \alpha^{-ak} \mod p$. A then unciphers the sent message by computing $m' = x \cdot \sigma \mod p$ (we indeed have that $m' = \alpha^{-ak} \cdot m \cdot \alpha^{ak} = m$).

You are B, and you receive the following public key from A (17,3,12) :

- Encrypt the message "2" by choosing some random number k.
- Using α and $\alpha^a \mod p$, find a.
- Apply the decryption algorithm to find the original message m.