TD n° 3 - Cryptographie

Solutions

Exercice 1 – Soit l'entier n, le produit de deux nombres premiers distincts p et q.

1. $\varphi(n) = (p-1)(q-1)$
2. Supposons que $n, \varphi(n)$ sont connus. Ainsi, on dispose d'un système de deux équations en p et q :

$$\begin{cases} pq = n, \\ p + q = n + 1 - \varphi(n). \end{cases}$$

qui donnent l'équation du second degré en X :

$$X^2 - (p+q)X + pq = 0$$

qui a comme racines p et q :

$$p = \frac{n + 1 - \varphi(n) + \sqrt{\big(n + 1 - \varphi(n)\big)^2 - 4n}}{2}$$

$$q = \frac{n + 1 - \varphi(n) - \sqrt{\big(n + 1 - \varphi(n)\big)^2 - 4n}}{2}$$

Exercice 3 – La clé publique de Bob ($n = 253, e = 13$).

1. $\varphi(n) = (p-1)(q-1) = 10 \times 22 = 220$.
   On trouve l'exposant sécret de Bob : $de = 1 \mod \varphi(n)$

$$13d = 1 \mod 220 \Leftrightarrow d = 17 \mod 220.$$

2. $C = M^e \mod n$: $C = 2^{13} = 96 \mod 253$.
3. $M = C^d \mod n$: On remarque que $22^2 = -22 \mod 253$ et $(-22)^2 = 22^2$.

$$M = 22^{17} = (22^2)^8 \times 22 = -22 \times 22 = -22^2 = 22 \mod n = 253$$

.