USTHB Faculté d'Informatique **Master M1 IL**

Epreuve de Sécurité Informatique

Question 1. Donner une définition de la sécurité (confidentialité) parfaite. Donner une de ses caractérisations. Y a-t-il une réalisation de cette sécurité parfaite ?

Question 2. Donner le principe du test de Kassiski pour la cryptanalyse de systèmes poly alphabétiques.

Question 3. Expliquer la notion de système itéré sur l'exemple du produit des cryptosystème multiplicatif et du décalage ou de César. Dans quel type de cryptosystème le trouve t-on ? Quel est son intérêt ?

Question 4. Chiffrer le texte **SECURITE INFORMATIQUE** avec le chiffrement par permutation transposition et la clé

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{pmatrix}$$

. Comment implémenter ce type de chiffrement avec le chiffrement matriciel ?

Question 5.. L'une des attaques (théoriques) sur le système RSA est la factorisation du modulus n. Montrer commment procéder à ce type d'attaque à l'aide de la technique (« grossière ») rho de Pollard, si $n = 247$. Expliquer le principe de cet algorithme. On choisira $a = 2, b = 5, f(x) = x^2 + 1 \, mod \, n$. Pourquoi le fait de trouver un facteur non trivial de n permet-il de « casser » le RSA ?

Mai 2024