USTHB

Master IL

Epreuve de rattrapage
de Sécurité

Question 1.

(i) Dans quel contexte rencontrons nous la notion de système itéré.
(ii) Expliquer cette notion avec des exemples simples de cryptosysèmes (le chiffrement multiplicatif et le décalage).

Question 2.

(i) Rappeler le principe du chiffrement RSA.
(ii) Pourquoi est-il réputé sûr ?
(iii) Chiffrer le message clair $x = 9453$ .avec un RSA avec $p = 101$, $q = 113$ et $b = 3533$.

Question 3.

(i) A quoi servent les tests de primalité?
(ii) Quel est leur rôle dans la factorisation ?
(iii) Expliquer le principe de la conception des algorithmes probabilistes de primalité ; des algorithmes déterministes de primalité prouvée.
(iv) Donner les algorithmes correspondants dans le cas général ou sur un exemple.

Question 4.

(i) Donner le principe et l'algorithme de calcul du logarithme discret.
(ii) Dans quel contexte avons-nous rencontré en cours et en TD ce type d'algorithmes ?

Juin 2024