Université Abderrahmane MIRA – Béjaia
Faculté de Technologie
Département de Génie Électrique
Filière : Télécommunication, Spécialité : Systèmes de Télécommunications

20 Mars 2021
Durée: 02H00

Concours d'accès au Doctorat (D/ LMD)

Epreuve : Traitement de l'Information

Partie 1: Cryptographie (08 pts)

Alice veut envoyer un message chiffré à Bob en utilisant le chiffrement RSA, mais ne connaît pas la clé publique de Bob. Alors, elle envoie à Bob un e-mail en demandant sa clé publique. Bob répond à l'e-mail en envoyant sa clé publique RSA qui est ***(e, N)***.

Cependant, l'opposant actif, Oscar, intercepte le message et change d'un bit l'exposant ***e*** de ***0*** à ***1***, donc Alice reçoit un e-mail affirmant que la clé publique de Bob est(e', N), où e' diffère de ***e*** avec un bit. Alice chiffre son message ***m*** avec cette clé et l'envoie à Bob. Bien sûr, Bob ne peut pas déchiffrer, car le message a été chiffré avec la mauvaise clé. Alors il renvoie sa clé une autre fois et demande à Alice d'envoyer à nouveau le message chiffré, donc c'est qu'elle a fait. L'opposant écoute encore l'ensemble de la communication sans interférer davantage et n'effectue aucune modification.

1. Démontrer comment l'opposant, Oscar, peut maintenant récupérer le message chiffré ***m*** de Alice ?

Partie 2: Traitement du signal (12 pts)

Soit un filtre numérique décrit par l'équation aux différences :

$$y(n) = 0{,}5\ x(n) + 0{,}5\ x(n-2)$$

1. Detreminer la fonction de transfert de ce filtre.
2. Déterminer sa réponse impulsionnelle.
3. Etudier la stabilité et la causalité du filtre, quelle est sa nature (justifier).
4. Déterminer sa réponse fréquentielle
5. Detreminer son spectre d'amplitude et de phase.
6. Quelle est la forme du spectre d'amplitude (entre $-0{,}5\ f_e$ et $0{,}5\ f_e$), donner la nature du filtre ainsi que les fréquences de coupure en fonction de f_e.