Université Badji Mokhtar - Annaba
Faculté des Sciences
Département d'Informatique
Année d'Etude : 2eme Année Master
Durée : 1 :30H Le 16/01/2022

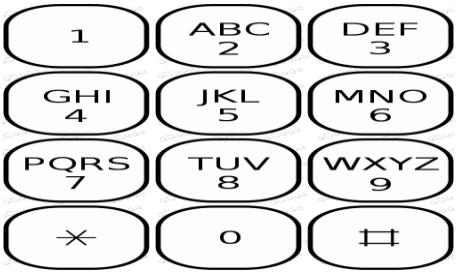
Cryptographie et sécurité des systèmes informatiques

Exercice1 : Chiffrez le message suivant TANGENTE EST UN SUPER MAGAZINE avec le code de Vigenère , vous utilisez la clef PORT. (3 pts):

IOEZT BKXTG KNCGL ITFDT VOQBCS

Exercice 2 : Mon prénom a été codé en utilisant les chiffres notés sur les touches d'un téléphone portable. Retrouvez mon prénom. Code : 66835683. (3 pts):

NOUDJOUD



Exercice 3 :

Alice envoie à Bob un message chiffré par sa clé Ka, Bob chiffre à son tour le message reçu avec sa clé Kb et le retourne à Alice. Comme le chiffrement est commutatif Alice peut déchiffrer le message et envoyer à Bob {m}Kb, message que Bob est alors capable de déchiffrer pour avoir le secret m.

1. Concevoir le protocole qui pourrait être entre Alice et Bob.
2. A quelle attaque ce protocole ne résiste-t-il pas ?
3. Donnez le scénario d'attaque.
4. Considérons une instance particulière de ce protocole, ou la communication entre Alice et Bob est comme suit :

   A→B : m ⊕ Ka

   B→A : m ⊕ Ka⊕Kb

   A→B : m ⊕ Kb

Expliquer quel type d'attaque le pirate peut tenter pour avoir le secret m et pourquoi une telle attaque est possible.

5. Maintenant, Alice souhaite transmettre une clef secrète Kab à Bob. Pour cela, elle envoie la clef Kab à un serveur de confiance, chiffrée à l'aide d'une clef Kas, ce que nous notons {Kab}Kas. Le message envoyé au serveur prend la forme :

   Alice, Bob, {Kab}Kas

   La clef Kas est partagée avec le serveur qui retrouve donc la clef Kab et la crypte avec Kbs, une clef qu'il partage avec Bob. Celui-ci récupère ainsi la clef Kab.
   - Donnez un scénario d'attaque.

Université Badji Mokhtar - Annaba
Faculté des Sciences
Département d'Informatique
Année d'Etude : 2eme Année Master
Durée : 1 :30H Le 16/01/2022

Cryptographie et sécurité des systèmes informatiques

1. Concevoir le protocole qui pourrait être entre Alice et Bob. (2 pts)

   A→B : {m}Ka

   B->A : {{m}Ka}Kb

   A→B : {m}Kb

2. A quelle attaque ce protocole ne résiste-t-il pas ? (2 pts):

   Les participants ne vérifient pas l'authenticité de l'identité de leurs correspondants, attaque Man in the middle ou homme au milieu peut être menée dans ce cas.

3. Donnez le scénario d'attaque. (2 pts)

   A→I(B) : {m}Ka

   I(A)->B :{m}Ka

   B→I(B) : {{m}Ka}Kb

   I(B)→A : {{m}Ka}Ki

   A->I(B) : {m}Ki

   A→I(B) : {m}Kb

4. Considérons une instance particulière de ce protocole, ou la communication entre Alice et Bob est comme suit :

   A→B : m ⊕ Ka

   B→A : m ⊕ Ka⊕Kb

   A→B : m ⊕ Kb

Expliquer quel type d'attaque le pirate peut tenter pour avoir le secret m et pourquoi une telle attaque est possible.
Failles d'implantation, Cas où un intrus profite des faiblesses dues à la combinaison de l'algorithme de chiffrement et du protocole cryptographique. Pour obtenir le secret m, un intrus peut intercepter les trois messages et exécuter le calcul suivant (3 pts):

Message1 ⊕ message2⊕ message 3 = m ⊕ Ka⊕ m ⊕ Ka⊕Kb⊕ m ⊕ Kb

= (m ⊕ Ka)⊕ (m ⊕ Ka)⊕ Kb⊕ m ⊕ Kb

=0⊕ Kb⊕ m ⊕ Kb

=Kb⊕ Kb⊕ m

Université Badji Mokhtar - Annaba
Faculté des Sciences
Département d'Informatique
Année d'Etude : 2eme Année Master
Durée : 1 :30H Le 16/01/2022

Cryptographie et sécurité des systèmes informatiques

$=0 \oplus m$

$=m$

5- Un attaquant I peut intercepter le message d'Alice destiné à Bob ;

Alice, Bob, {kab]kas et envoyer le message :

Alice, I, {kab]kas à la place, le serveur croit alors qu'Alice souhaite transmettre le message à I et envoie le message : Alice, I, {kab]kis à I, qui peut alors avoir le clé kab. (2 pt)

Exercice 4 : Appliquer la méthode Playfair pour chiffrer votre nom de famille avec le mot clé « MASTER ». (3 pt) matrice + chiffrement

M	A	S	T	E
R	B	C	D	F
G	H	I/G	K	L
N	O	P	Q	U
V	W	X	Y	Z