École Polytechnique de Montréal

Département de génie informatique et génie logiciel

INF4420A

Rapport travail pratique 1 - Session A20

TP1

Lucas Aubrun, 2035618

Paul Clas, 1846912

Table des matières

1 Partie A

1.1

1.2

1.3

1.4

2 Partie B

2.1

a) Le texte issu de la source correspond aux chiffres entrés par l'utilisateur du guichet, donc s est en ASCII. Le codeur transforme ensuite ces chiffres en bloc de 8 octets, donc t est en binaire. Lors du chiffrement DES, les bits sont permutés et substitués, mais l'alphabet obtenu reste du binaire. Donc t' est en binaire.

b)Les langages provenant de s sont toutes les combinaisons de 4 chiffres chacun entre 0 et 9 (0000 à 9999). Les langages provenant de t et de t' sont toutes les combinaisons binaires sur 64 bits.

c)Nous avons identifiés les quatres attaques suivantes auxquelles le système est vulnérable :
- Attaque "Man in the middle"
- Attaque par rejeu
- Attaque à texte clair connu
- Attaque par force brute

Les messages sont envoyés par réseau, donc le système est exposé à une attaque "Man-in-the-middle". À partir de là, l'attaquant peut modifier les messages pour empêcher l'utilisateur de changer son code NIP, il peut enregistrer le message pour se connecter plus tard au compte client par rejeu ou il peut essayer de décoder le messager pour voler des informations bancaires.
En effet, il y a 10^4 possibilités pour le code NIP, donc 10^4 messages différents peuvent être envoyés à l'ordinateur central, car le code NIP est composé de 4 valeurs entre 0 et 9 et il est répété 2 fois pour détecter les erreurs de transmission. Le système est donc vulnérable a une attaque par force brute, car il y a relativement peu de possibilités.
Par ailleurs, la clé de chiffrement est fixée et l'algorithme DES est utilisé, donc le système est vulnérable à une attaque à texte clair connu.

d)

- Man-in-the-middle : L'attaquant
- Attaque par rejeu : L'attaquant capte le code NIP chiffré, il l'enregistre et il pourra le réutiliser pour se connecter (depuis la même position) au compte du client. Cette attaque fonctionne car la clé de chiffrement du système est fixe, donc le message chiffré que recevra l'ordinateur central sera toujours le même.
- Attaque à texte clair connu : L'attaquant peut se créer un compte bancaire afin d'avoir son propre code NIP (connu). Il peut ensuite intercepté son code NIP après chiffrement. La clé étant fixe et l'algorithme de chiffrement utilisé étant DES, il pourra retrouver la clé de chiffrement du système.
- Attaque par force brute : L'attaquant peut intercepté le code NIP chiffré et, comme il connaît le fonctionnement de la boîte de codage, il peut le décoder par force brute car il n'y a que $10^4 possibilits$ (4 chiffres entre 0 et 9, dédoublés).

e)

— Codage 1 :

2.2

a) Le protocole HTTPS opère sur une connection encryptée à l'aide de SSL ou de TLS. La différence dans l'url est la présence du s dans https ://desjardins.com à la différence de http ://desjardins.com [**1**]. On peut même observer des îcones différents apparaitre dans le navigateur web : b)

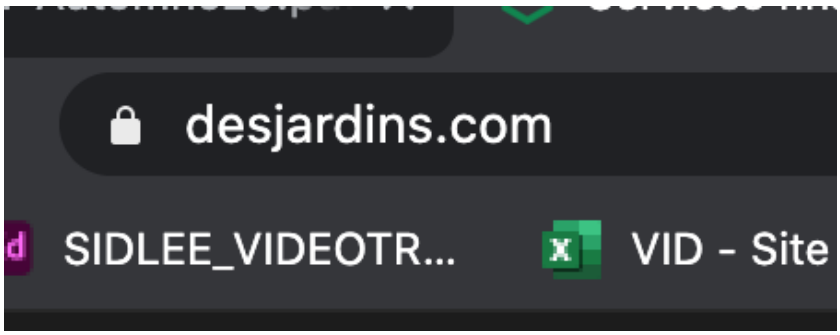

FIGURE 1 – Îcone d'un site web utilisant le protcole HTTPS dans le navigateur Chrome

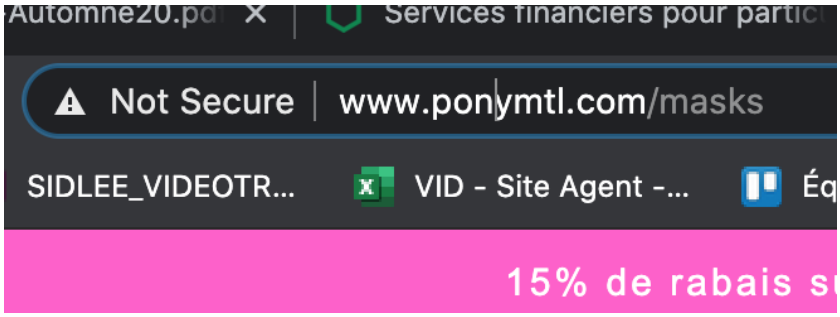

FIGURE 2 – Îcone d'un site web utilisant le protcole HTTP dans le navigateur Chrome

2.3

a)
Le chiffrage en mode ECB permet de masquer légèrement le mot de passe écrit sur l'image original, mais il est toujours visible à l'oeil nu.

b) Le chiffrage en mode CBC permet de masquer complètement le mot de passe pour l'oeil : il ne peut plus être lu simplement et doit être déchiffré. c)

2.4

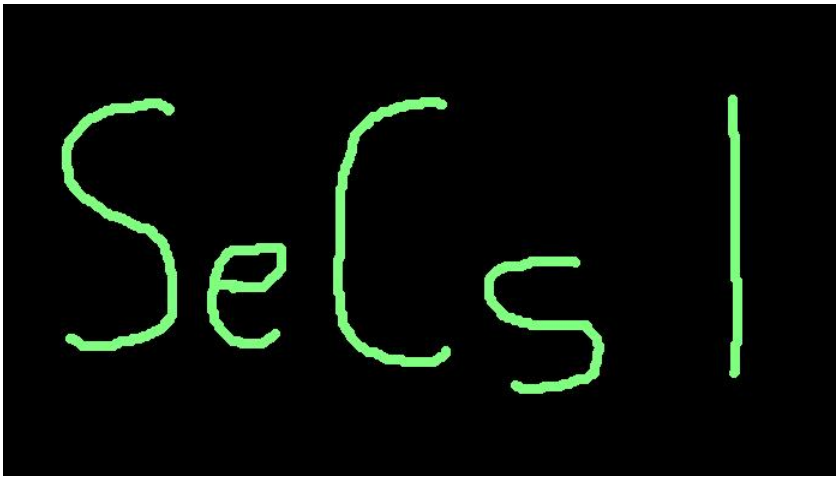

FIGURE 3 – Fichier mdp.jpg original

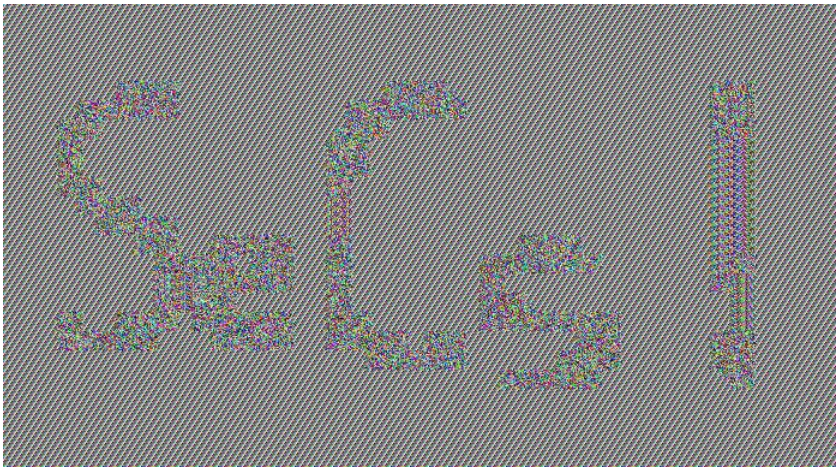

FIGURE 4 – Fichier mdp.jpg chiffré en mode ECB

FIGURE 5 – Fichier mdp.jpg chiffré en mode CBC

3 Partie C