Table des matières

Introduction

Candidat "Officier de carrière" à l'***École Royale Militaire*** (ERM), je suis actuellement ma formation académique à l'***École Centrale des Arts et Métiers*** (ECAM) en option électronique.

Durant notre 2ème année de Master, les étudiants doivent réaliser un stage d'immersion en entreprise d'une durée de 6 semaines. Ce stage consiste, entre autres, à s'insérer dans une entreprise afin d'y découvrir différents aspects tels que l'organisation générale d'une entreprise, son management, son contexte social, son insertion économique, ses aspects techniques et ses produits. Il a également pour but de se familiariser au travail quotidien de l'ingénieur en participant à diverses activités.

Ayant réalisé mon stage de 3ème Bachelier chez ***AIRBUS DS SLC*** sur le site de Diegem et de Elancourt, il était important pour moi de saisir la chance et l'opportunité de découvrir une nouvelle entreprise renommée à travers le monde. C'est ainsi que je décidai de réaliser mon stage chez ***THALES*** *Telecommunications Belgium* sur le site de Tubize.

1 Environnement de stage

Cette section a pour objectif de décrire l'entreprise à différents points de vue. Tout d'abord, une description de la structure de l'entreprise (dont l'équipe dans laquelle se trouve le stagiaire) et de ses objectifs est reprise. Ensuite, sont détaillées succontement la gestion de production mais aussi la gestion marketing, la gestion financière et la gestion des ressources humaines. Enfin, un descriptif de la cellule qualité clôturera ce premier point.

1.1 Structure de l'entreprise

C'est donc chez ***Thales*** *Telecommunication Belgium* que je me suis rendu pour réaliser mon stage d'immersion en entreprise.

1.2 Objectifs de l'entreprise

1.3 Equipe du stagiaire

1.4 Gestion de production

1.5 Gestion marketing

1.6 Gestion financière

1.7 Gestion des ressources humaines

1.8 Politique QHSE

2 Objectifs du stage

L'objectif de ce stage était d'introduire l'ensemble des notions élémentaires, nécessaires pour la réalisation du *Travail de Fin d'Étude* (TFE). Ce travail de fin d'étude qui allait se poursuivre durant 6 mois à compter du mois de Novembre 2018. Dans un premier temps, une définition des notions théoriques est abordée. Ensuite, un exemple ou une simulation est mise en oeuvre afin d'appuyer le concept théorique.

La liste ci-dessous reprend l'ensemble des objectifs fixés et réalisés durant les 6 semaines de stage :

1. **Notions de chiffrement et de *Side-Channel Attacks* (attaques par canal auxiliaire)**
2. **L'algorithme AES (*Advanced*)**
3. **Simulation d'un tracé et d'une attaque par canal auxiliaire sur MATLAB**
4. **Notions de statistiques et de t-test**
5. **Simulation d'un t-test sur MATLAB**

Ces différents objectifs sont décrits dans la section 3 *"Projet du stage"*.

3 Projet du stage

Cette section décrit l'ensemble des objectifs, cités à la section 2, fixés pour le stage.

3.1 Notions de chiffrement et de *Side-Channel Attacks*

Les systèmes de sécurité modernes utilisent des algorithmes de chiffrement pour assurer la disponibilité, la confidentialité et l'intégrité de données. Ces algorithmes de chiffrement sont en réalité des fonctions mathématiques qui prennent typiquement :

— 2 paramètres en entrée : un ***message clair*** (nommé *plaintext* en anglais) et une ***clé de chiffrement*** (nommé *key* en anglais).
— 1 paramètre en sortie : le ***message chiffré*** (nommé *ciphertext* en anglais).

Le procédé transformant les données claires en entrée en données chiffrées en sortie est appelé le ***chiffrement***. Ce procédé est réalisé grâce à un ***algorithme de chiffrement*** utilisant une clé de chiffrement et diverses opérations mathématiques. Il est important de préciser que tous les détails décrivant le fonctionnement d'un algorithme sont disponibles publiquement, seule la clé de chiffrement doit rester secrète.

La figure 1 ci-dessous présente le principe de fonctionnement d'un algorithme de chiffrement.

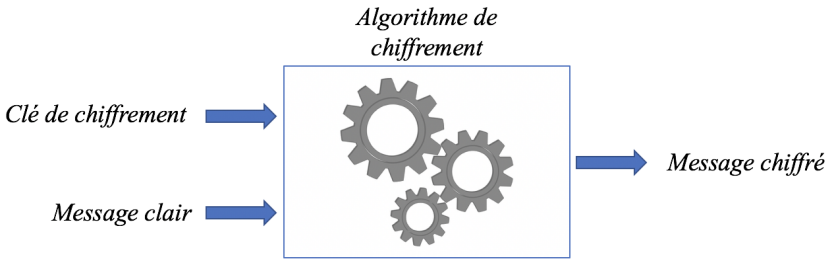

Figure 1 : L'algorithme de chiffrement, caractérisé par diverses opérations mathématiques, utilise une clé de chiffrement en entrée pour chiffrer un message clair. Cela produit un message chiffré, non compréhensible pour une personne ne connaissant pas la clé de chiffrement.

Nous distinguons 2 types d'algorithmes de chiffrements :

— ***Chiffrement symétrique*** : Le chiffrement est dit symétrique lorsque le procédé de chiffrement (algorithme) utilise une seule clé, appelée *clé secrète*. Par convention, ce type de chiffrement permet à la fois de chiffrer et de déchiffrer des messages à partir d'une seule et unique clé. Le désavantage de ce typer de chiffrement est que si une personne parvient à subtiliser la clé publique, elle sera en mesure de déchiffrer tout message qu'elle intercepte.
Exemple : L'algorithme AES.

— ***Chiffrement asymétrique*** : Le chiffrement est dit asymétrique lorsque le procédé de chiffrement (algorithme) utilise 2 clés : une *clé publique* et une *clé privée*. Par convention, la clé publique est la clé de chiffrement du message clair, elle peut être communiquée sans aucune restriction tandis que la clé privée est la clé de déchiffrement du message chiffré, elle ne doit être communiquée sous aucun prétexte. Le fonctionnement est le suivant : Avec une clé publique, l'expéditeur code, dans un algorithme de chiffrement donné, un message. Ce message, une fois transmis, ne pourra être déchiffré que par le destinataire, détenteur de la clé privée.
Exemple : L'algorithme RSA.

Les figures 2 et 3 ci-dessous présentent les principes de fonctionnement des chiffrements symétriques et asymétriques.

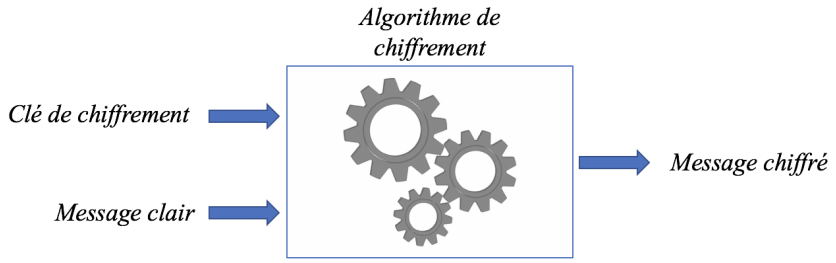

Figure 2 : Chiffrement symétrique : Une seule clé est utilisée pour chiffrer et déchiffrer les messages.

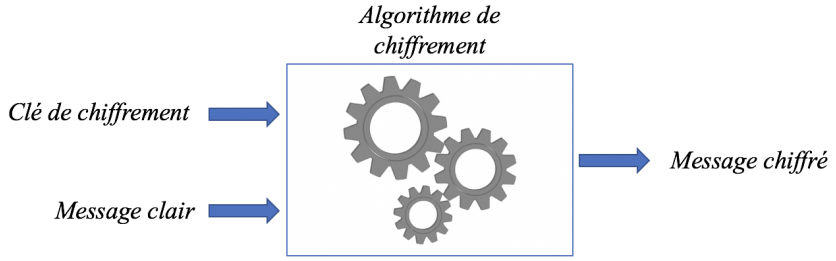

Figure 3 : Chiffrement asymétrique : Un clé publique est utilisée pour chiffrer le message et une clé privée est utilisée pour le déchiffrer.

3.2 Algorithme AES

3.3 Simulation d'un tracé et d'une attaque par canal auxiliaire sur MATLAB

Afin de bien assimiler les notions de *side-channel attacks*, il m'a été demandé de réaliser une simulation sur MATLAB. La première phase de la simulation génère des traces sur base de l'algorithme AES. La seconde phase de la simulation est une attaque par canal auxiliaire. Plus précisément, cette attaque est réalisée sur un seul byte de donnée et se fait en sortie de la SBox. Ce type d'attaque est appelé CPA. Pour cette raison, seules les 2 premières étapes de l'algorithme AES sont nécessaires et seront donc simulées (*AddRoundKey()*, *SubBytes()*).

3.4 Notions de statistiques et de t-test

3.5 Simulation d'un t-test sur MATLAB

4 Conclusion

Crédits

— Figure **??** provenant de :
Le blog officiel de Texas Instrument : https://e2e.ti.com/blogs_/archives/b/precisionhub/archive/2015/01/21/delta-sigma-adc-basics-understanding-the-delta-sigma-modulator
— Figure **??** provenant de :
Par Yves-Laurent (Travail personnel) [GFDL (http://www.gnu.org/copyleft/fdl.html), CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/)], de Wikimedia Commons
— Figure **??** provenant de :
Par Inductiveload (Travail personnel) [Public domain], de Wikimedia Commons
— Figure **??** provenant de :
Par Toriicelli (Travail personnel) [Public domain], de Wikimedia Commons
— Figure **??** provenant de :
Par Daniel Braun [GFDL (http://www.gnu.org/copyleft/fdl.html), CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/) ou CC BY 2.5 (https://creativecommons.org/licenses/by/2.5)], de Wikimedia Commons