INFO-F-405 – Sécurité Informatique
Projet 1 : 2-DES

Année académique 2010-2011

1 Introduction

Le `DES` (Data Encryption Standard) est un algorithme de chiffrement intensivement utilisé durant ces trente dernières années. Il est aujourd'hui encore régulièrement utilisé sous la forme `3-DES` (chiffré $=E_{k_3}(D_{k_2}(E_{k_1}(x)))$).

Nous vous invitons à vous intéresser à la construction de 2-DES : chiffré $= E_{k_2}(E_{k_1}(x))$. L'algorithme `2-DES` est simple : il consiste en l'exécution consécutive de deux DES avec deux clés différentes de chiffrement sur un texte clair de départ (voir Figure 1).

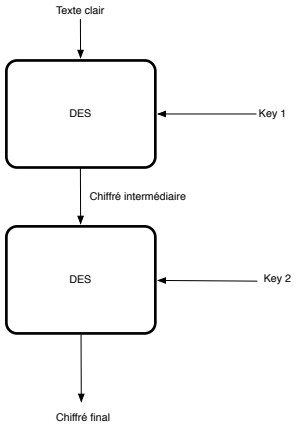

FIGURE 1 – Schéma d'implantation du 2-DES

2 Question 1

En vous basant sur le code de DES (provenant d'une librairie cryptographique) nous vous demandons d'implémenter `2-DES`, sous la forme d'un objet qui devra être utilisable comme s'il faisait partie d'une librairie cryptographique. La classe représentant l'objet se nommera `2-DES` et devra posséder une méthode `init(k1,k2,IV)` qui initialise l'algorithme avec les deux clés et le vecteur d'initialisation, une méthode `encrypt(.)` qui prendra un nom de fichier en paramètre et le chiffrera, et une méthode `decrypt(.)` qui déchiffrera un fichier dont le nom est passé en paramètre de la fonction. Lorsqu'un message clair devra être chiffré avec votre 2-DES, ce chiffrement devra être réalisé en mode CBC (*Cipher Block Chaining*) dont le vecteur d'initialisation (IV) sera 0 [1]. Vous devez réaliser cette implantation en Java ou en Python. En fonction de votre choix de langage vous utiliserez soit l'API standard *"crypto"* de Java (contenu notamment dans les classes

1. En général, les librairies cryptographiques vous demanderont de passer un string composé de zéros en paramètre

`javax.crypto`), soit la bibliothèque `PyCrypto` (disponible sur *http ://www.dlitz.net/software/pycrypto/*) pour Python.

3 Question 2

Nous vous demandons ensuite de vous mettre dans la peau d'un cryptanalyste et d'implémenter une attaque à texte clair connu *"meet-in-the-middle"* : connaissant deux textes clairs x_1 et x_2 et les deux textes chiffrés correspondants y_1 et y_2 (obtenus au moyen de la même paire de clé), l'objectif est de retrouver les deux clés utilisées pour chiffrer. Pour ce faire vous devez calculer $E_{k_1}(x_1)$ pour toutes les clés k_1 possibles et sauvegarder les résultats ; puis vous calculez $D_{k_2}(y_1)$ pour toutes les clés k_2 possibles. Toutes correspondances entre les éléments des deux ensembles de résultats ainsi produits correspondent à des paires de clés qui pourraient être les clés cherchées ; les paires de clés potentielles sont testées en vérifiant si $y_2 = E_{k_2}(E_{k_1}(x_2))$. Pour cette question, pour des raisons de praticabilité, seuls 16 bits des 56 bits [2] de la clé seront variables (les 40 bits de poids forts de chaque clé considérée seront toujours égaux à 0) [3]. Nous vous demandons aussi d'indiquer quelle est la complexité (en grand O) de cette attaque.

4 Modalités de réalisation

Le projet est à faire par groupe de 3 personnes. Vous devrez rendre un listing complet de vos implantations ainsi qu'un bref rapport de quelques pages nous expliquant vos choix d'implantations, les avantages et inconvénients de ces derniers, ainsi qu'une analyse de la méthode d'attaque que vous avez utilisée contre `2-DES`.

Nous vous demandons de nous fournir une version papier au secrétariat du département d'informatique reprenant vos noms et votre numéro de groupe. Vous enverrez aussi à l'adresse e-mail `infof405@lit.ulb.ac.be`, une version électronique de votre projet. Votre projet devra être contenu dans un dossier compressé au format `zip`. Le format de nom du dossier est `Secu` + votre numéro de groupe + le langage utilisé (Exemple : `Secu3Java.zip`, ou `Secu4Python.zip`). Suite à la remise de votre projet, nous organiserons une défense orale dont la date et le planning de passage seront communiqués aux valves et à vos délégués.

2. Dans certaines bibliothèques, l'implantation de DES requiert un clé de 8 octets (64 bits), car elles prennent en compte les bits de parités.

3. Cette dernière restriction vous permettra de tester votre attaque en un temps d'exécution raisonnable.

Consignes pour la remise du projet

À respecter scrupuleusement !

1. Votre projet doit indiquer **votre nom** et **votre numéro de groupe**.
2. Votre projet doit être **dactylographié**. Les projets écrits à la main ne seront **pas corrigés**.
3. Votre implantation doit être **commenté**.
4. Vous devez respecter les contraintes de langage et de bibliothèque.
5. Vous devez respecter les modalités suivantes :
   - Date limite de remise : **le 18 octobre 2010**
   - Lieu : **au Secrétariat « étudiants » du Département d'Informatique, local 2N8.104**
   - Heure : **Avant 16h**

   Le secrétariat ferme à 16h. **Après 16h**, les projets sont considérés comme **en retard**, et vous perdez **2 point** sur votre note finale (plus un point par jour ouvrable de retard). Les projets en retard doivent être déposés **dans la caisse** prévue à cette effet aux heures d'ouverture des jours suivants du secrétariat. Ces contraintes sont valables pour l'envoi de la version électronique du projet.