INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Cryptography

Projects *November 7th, 2016*

1. Description

1. **Bank application.** In this application a user must be able to manage his bank account online in a secure way. Whenever a user wants to establish communication with the bank, the application will generate a key session between the user and the bank using Diffie-Hellman protocol based on elliptic curves (ECC). The key session will be used to encrypt all the communication between the user and the bank. The key session must be adequate to work with AES (considering 12 rounds) and a mode of operation (CBC, CTR). For each user the system will maintain his name, an id of 8 digits and a password (*passwd*). A user will access the system using his id and password, both data must travel encrypted whenever a user wants to establish communication to the bank. The system will store $h(passwd)$, where h will be SHA-1. To manage the information the users and their accounts we will maintain a database. There will be two kinds of accounts:

   - **Saving account.** For this account there will be an account number, the balance, withdrawals and deposits and the corresponding dates.
   - **Credit account.** For this account the system will store the credit card number, the total credit that the user has, the balance, the payments and the charges done to the credit card, and the corresponding dates

   Any user must have at least a saving account, and at most a saving account and a credit account. He must be able to do the following:

   - To check the transactions in a period of time of his accounts.
   - To make transfer between his own accounts
   - To make transfer to other users in the same bank, to do this he will need the account number or the credit card number and the name of the owner

   This project must be done for a team of 4 students

2. **Digital Sealed Envelope I**. In this project you will use a AES with 12 rounds and 3DES with 12 rounds joint to encrypt a file. Everytime that you encrypt a file you will need to generate a new key K and choose a mode of operation (CBC,CTR). Then you will encrypt this key K, using a small version of elliptic curve cryptosytem (ECC). You must consider, that each user must have two keys: a private and a public. **This project must be done for a team of 4 students**. You must consider the following requirements.

    - Key generation for AES and 3DES. Your application must offer the option to generate a key k at random. You must find a way to automatically know if the key was generated of AES or for 3DES.
    - Encryption/Decryption with AES and 3DES. In this case your application must be able to encrypt/decrypt any file of any length. The user can choose the mode of operation. Any information associated with the mode of operation, must be randomly generated, and store in the ciphertext.
    - Key Generation for elliptic curve cryptosystem There must be an option to generate a pair of keys: public and private. Again some parameters must be randomly generated. The private key must be stored in a file with extension .ecc The public keys must go to a file which we call key ring. This file will store the public keys for several users, thus it must contain other data: the full user name, and the expiration date.
    - Encrypting K (of 3DES or AES) with ECC. The symmetric key must be encrypted with the public key of the receiver. This encrypted key must be added to the ciphertext generated by AES or 3DES.
    - Decrypting K (of 3DES or AES) with ECC. To decrypt the application must ask the user the filename of his/her private key. The application will take the encrypted key included in the ciphertext, it will decrypt it using the private key. Then it will decrypt the ciphertext with the K.

2. Products

To check the advances in your project, we will do the following

1. On November 15th and 22nd you must show advances on those parts of your system that use symmetric key encryption.
2. On November 29th and December 6th there will be an interview with each team,

where the team must be able to explain how to generate keys, encrypt and decrypt in an elliptic curve cryptosystem.

3. From December 8th to 15th each team will do a presentation of the application. Each team will have 20 minutes to present. **You will be able to present only if you are authorized to do so. Each team can get this authorization only after I have reviewed your slides and the user's manual and you have done the corresponding corrections (if there are any).**