Estructuras de Datos

CRIPTOGRAFÍA

ACTIVIDAD A-6.1: CRIPTÓGRAFO

René Ornelis

Vacaciones de junio de 2024

Criptografía

1 Objetivos

Los objetivos de esta actividad son que el estudiante sea capaz de:

1. Aplicar la criptografía sin necesidad de saber los detalles de los algoritmos de encripción.

2 Problema

La encriptación de extremo a extremo es una medida de seguridad fundamental en el ámbito de la comunicación digital. Se refiere al proceso de cifrar la información de manera que solo el emisor y el receptor autorizados puedan acceder a su contenido, asegurando que nadie más, incluidos posibles intermediarios o terceros, pueda interceptar o entender la información transmitida. La importancia de la encriptación de extremo a extremo radica en la protección de la privacidad y la confidencialidad de la información en un mundo cada vez más conectado digitalmente que cobra relevancia para conservar la privacidad del usuario, protección contra intercepciones malintencionadas, seguridad en transacciones financieras y otros.

Dada la siguiente clase:

```
class Criptografo {
public:
  Criptografo (string llvPub, string llvPriv) ;

  /** genera el criptograma para enviar un mensaje certificado usando las
llaves propias y la llave del destinatario llvDestinatario */
  string enviar (string llvDestinatario, string mensaje) ;

  /** Recibe un criptograma certificado usando las llaves propias y la llave
del remitente llvRemitente y genera el mensaje recibido*/
  string recibir (string llvRemitente, string criptograma) ;
private:
  string llvPublica, llvPrivada ;

  /** devuelve el criptograma correspondiente a la encripción RSA del mensaje
con la llave llv pública o privada */
  string encriptaRSA(string llv, char *mensaje) ;

  /** devuelve el mensaje correspondiente a la desencripción RSA del
criptograma con la llave llv pública o privada */
  string desencriptaRSA (string llv, string criptograma) ;

  /** devuelve el criptograma correspondiente a la encripción AES del mensaje
con la llave llv pública o privada */
  string encriptaAES(string llv, char *mensaje) ;

  /** devuelve el mensaje correspondiente a la desencripción AES del
criptograma con la llave llv pública o privada */
  string desencriptaAES (string llv, string criptograma) ;
```

```
  /** genera una llave de sesión aleatoria */
  string sesion() ;
}
```

Implemente el proceso de encripción extremo a extremo (E2E) de forma que una persona X envíe un mensaje a una persona Y, de modo que X esté seguro de que sólo Y podrá leer el mensaje y Y esté seguro que sólo X pudo haber enviado el mensaje, a través de desarrollar:

a. El método ***enviar()*** *y el* método ***recibir()*** (en archivo Criptografo.cpp)
b. El programa que usará X para encriptar el mensaje (en archivo x.cpp)
c. El programa que usará Y para desencriptar el mensaje (en archivo y.cpp)

El proceso E2E debe optimizar el uso del procesador a través de minimizar la aplicación de encripción asimétrica.

Puede suponer que ya están implementados los métodos *encriptaRSA(), desencriptaRSA(), encriptaAES(), desencriptaAES()* y *sesion()* y que cada programa (X y Y) obtendrán las llaves privadas y públicas de una base de datos o archivo de configuración.

2.1 Restricciones

- No se permite agregar variables a las clases
- No se permite cambiar la visibilidad de los miembros de la clase
- Cualquier método que invoque en su solución, debe desarrollarlo.
- No se permite cambiar la interfaz de los métodos público.

3 Tiempo de entrega

La entrega se debe realizar en la plataforma de la Facultad o, en caso de que esta no esté disponible, por correo electrónico, a más tardar el 26/abril a las 09:00. No se permitirá entregas posteriores al límite definido.

4 Entregables

Deberá entregar archivo ZIP con los siguientes archivos fuentes compilables:

1. Criptografo.h: definición de la clase Criptografo.
2. Criptografo.cpp: implementación de la clase Criptografo
3. X.cpp: Programa de envío que utilizará el remitente para encriptar y enviar.
4. Y.cpp: Programa de recepción que utilizará el destinatario para desencriptar y recibir la información.

5 Criterios de evaluación

Objetivo	Puntos	Detalle por evaluar
Método enviar	1	Se implementa correctamente la encripción para enviar
Método recibir	1	Se implementa correctamente la encripción para recibir
Envío	1	Se aplica correctamente la clase por parte del remitente (x.cpp)
Recepción	1	Se aplica correctamente la clase por parte del destinatario (y.cpp)
TOTAL	4	