Estructura del protocol

Integrants

- Pau Bru Ribes
- Maria Arqués Vargas

Objectius

Comparar l'eficiència de dos mètodes d'encriptació/desencriptació de dades: AES i RSA, en termes de temps necessari per a encriptar i desencriptar uns arxius de diferents mides i contingut aleatori.

Intentarem determinar si existeix una diferència considerable en el temps d'execució d'ambdós protocols i analitzar com la mida dels arxius influeix en el rendiment de cadascun.

Aquest estudi ens permetrà determinar quin mètode és més eficient sota diferents condicions i així poder proporcionar una millor recomanació per al seu ús.

Variables Recollides

Resposta T

Temps emprat en l'encriptació/desencriptació.
Variable (Contínua) que volem comparar entre els diferents protocols.
Farem ús de la llibreria "<chrono>" de C++ per a mesurar-ho.
Inicialitzar el cronòmetre abans de cridar a la respectiva funció i es para quan retorna l'arxiu encriptat/desencriptat.

- **T_1** = Temps encriptació mesurat en segons.
- **T_2** = Temps desencriptació mesurat en segons.

Decisions P

Protocol d'encriptació utilitzat.
Variable (Categòrica) que defineix quin protocol hem fet servir.
Farem ús de la llibreria "<openSSL>" de C++ per a implementar els protocols.
Aquests protocols representen les diferents poblacions de l'estudi.

- **P_1** = AES-256 (Advanced Encryption Standard)
- **P_2** = RSA-256 (Rivest–Shamir–Adleman)

Co-Variables M

Mida de l'arxiu abans de l'encriptació en MB.
Variable (Contínua) que indica la mida inicial de l'arxiu que analitzem.
Permetrà analitzar la influència de la mida de l'arxiu respecte al temps emprat.
Es mesura obtenint la mida de l'arxiu abans d'encriptar l'arxiu.

- **M_1 =** Mida inicial (abans d'encriptar) de l'arxiu en MB.

Recollida de dades

1. **Preparació dels arxius**: Generar arxius de text amb contingut "pseudoaleatori" de diferent mida (1,5,10,50,100) MB. Suposarem que la llibreria "<openssl/rand.h>" té una implementació "suficient aleatòria" per a aquest estudi.
2. **Implementació dels algorismes**: Implementar els mètodes d'encriptació AES i RSA en C++ fent ús de les llibreries d'"OpenSSL". Suposarem que les implementacions d'aquests són eficients.
3. **Mesura del temps**: Configurar, amb l'ús de la llibreria "chrono" un cronòmetre previ a cada funció.
4. **Repeticions**: Per a minimitzar l'impacte de factors externs, repetir cada combinació "Mètode-Mida-Acció" un total de 10 vegades i així obtenir una mitjana més fiable.
5. **Emmagatzematge de resultats**: Tots els resultats s'han de registrar en un full de càlcul. Cada fila representa una possible combinació. Hi ha 10 columnes entre el nom de la combinació i la mitjana obtinguda on representa el temps empleat a cada repetició. Finalment, la mitjana és la suma de tots els temps per combinació dividida entre 10.

Combinació	**Repetició_i**	**Mitjana Obtinguda**
Mètode-Mida-Acció	temps en segons	temps en segons

6. **Condicions Externes**: Les proves s'han de realitzar en el mateix ordinador amb cap altra aplicació (Entenem que siguin d'usuari) en funcionament.

Mostra

Total d'observacions: (Núm. mètodes) * (Quantitat de mides) * (Núm. Accions) * (Repeticions) = 2*5*2*10 = **200 observacions**.

Tot i que suposem que les implementacions d'aleatorietat de les llibreries d'OpenSSL és molt bona, no podem assegurar que hi hagi la mateixa probabilitat a l'hora de generar els arxius. És per això que **no** es tracta d'una **mostra aleatòria simple**.

Les **dades** es consideren **aparellades**, ja que farem ús dels mateixos arxius per a comprovar els resultats, tot i que els **resultats** obtinguts seran **independents** perquè un mètode no influencia l'altre.