TEMPS D'ENCRIPTACIÓ

RSA-256 v.s. *AES-256*

Curs: 2024-25 Q3 PE
Integrants: Pau Bru, Maria Arqués

Índex

Introducció

Aquest informe **analitza** els **temps d'encriptació** de dos mètodes criptogràfics: *AES-256* i *RSA-256.*
L'objectiu principal és **comparar l'eficiència** en termes de temps emprat per ambdós mètodes a l'hora d'encriptar diversos **fitxers** de **diferents mides** amb contingut aleatori.
D'aquesta manera, avaluem si existeix una diferència entre protocols i com la mida dels fitxers afecta el rendiment.

Nota: Donat que els ordinadors no són capaços de generar nombres aleatoris, confiem en el fet que l'aleatorietat implementada en les llibreries usades és suficient. Realment hauríem d'emprar el terme pseudoaleatori quan parlem del contingut dels fitxers a encriptar.

Resum

Els resultats mostren que, de mitjana, **RSA-256** és entre **40** i **44 vegades més lent** que AES-256.
Mitjançant proves estadístiques inferencials (t-test aparellat sobre dades log-transformades), s'ha comprovat que la **diferència observada no** és **deguda** a l'**atzar**.
Les conclusions **recomanen** l'ús d'**AES-256** per a **fitxers grans**, donada la seva major eficiència.

Metodologia

Objectius

- **Comparar eficiència** de AES-256 i RSA-256 en termes de temps d'encriptació.
- **Determinar** si existeix **diferència** significativa entre els mètodes.
- **Analitzar** com la mida dels fitxers afecta el **rendiment** del protocol.
- **Verificar les premisses** necessàries per **aplicar** el **t-test** (aparallellat) i, si cal, aplicar transformacions per complir-les.

Variables Recollides

- Resposta (T): Temps empleat en l'encriptació. Mesurat en segons.
- Decisions (P): Protocol d'encriptació utilitzat.
    - P_1: AES-256 (Advanced Encryption Standard)
    - P_2: RSA-256 (Rivest-Shamir-Adleman)
- Co-Variables (M): Mida del fitxer abans de la seva encriptació. Mesurat en MB.

Recollida de Dades

1. **Preparació dels arxius**: S'han generat arxius de text amb contingut aleatori de mides [1,25] MB fent ús la llibreria "<*openssl/rand.h*>".
2. **Implementació dels algorismes**: S'han implementat els mètodes d'encriptació *AES-256* i *RSA-256* en C++ fent ús de les llibreries "<*openssl*>".
3. **Mesura del temps**: S'ha configurat un amb l'ús de la llibreria "<*chrono*>" un cronòmetre previ a la funció d'encriptació i es para quan retorna l'arxiu encriptat.
4. **Repeticions**: Cada combinació "Mètode-Mida" s'ha repetit 5 vegades per obtenir una mitjana més fiable.
5. **Emmagatzematge de resultats**: Tots els resultats s'han registrat en un full de càlcul. Cada fila representa una possible combinació "Mètode-Mida-Repetició-Temps".

Mètode P	**Mida** M	**Repetició**	**Temps** T
{AES-256, RSA-256}	MB	[1,5] Natural	Segons

6. **Condicions Externes**: Les proves s'han realitzat en el mateix ordinador amb cap altra aplicació en funcionament, assegurant que no hi hagi interferències externes.

Mostra

Mida de la mostra: Quantitat de mides diferents de fitxers a encriptar → **25**.

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.

Anàlisi Estadístic

S'han **calculat** els estadístics {**mitjana, desviació estàndard**} (No transformats) per a cada combinació "Mètode-Mida" i la mitjana conjunta de cada mètode: μ_{RSA} i μ_{AES}.
S'ha **calculat** l'estadístic "**Diferència**" tal que $\mu_D = \mu_{RSA} - \mu_{AES}$.

	Mitjana	**Desviació Estàndard**
AES-256	0.05140427	0.03123011
RSA-256	2.052867	1.133193
Diferència	2.001462	1.102195

La magnitud de la diferència és molt elevada, fet que ens fa sospitar d'un efecte multiplicatiu (el temps creix de forma no lineal amb la mida).

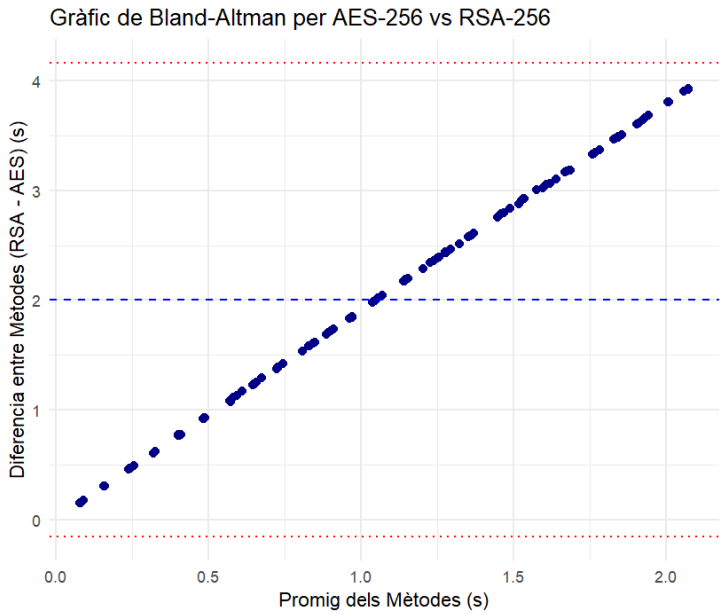
Validació de les Premisses

1. **Independència de les Observacions:**

Les **observacions** són **independents** perquè encriptar un fitxer amb un **mètode no afecta** de cap forma al **resultat posterior**. També s'ha procurat evitar encriptar dos fitxers alhora perquè no hi hagi interferències causades pel sistema operatiu.

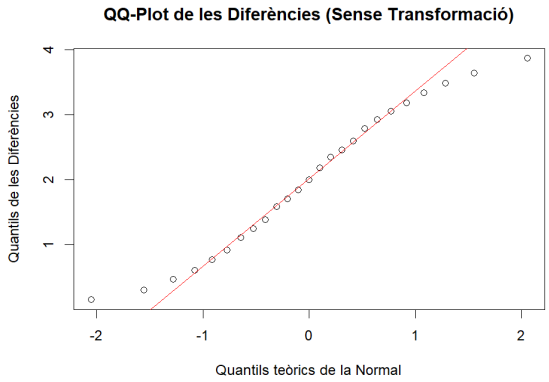
2. **Efecte Multiplicatiu**:

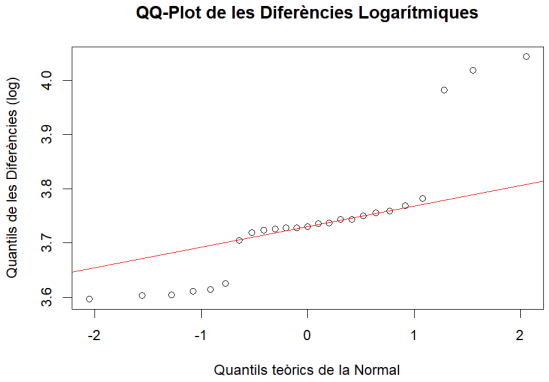
Donat que estem comparant temps entre protocols, el temps necessari per a encriptar augmentarà de forma exponencial a mesura que incrementi la mida.
Com podem observar en el gràfic de Bland-Altman, a mesura que la **mida augmenta**, **també** ho fa la **diferència** de **temps** entre els mètodes implicant així que estem davant un **efecte multiplicatiu**. És per això que tot índica que haurem d'aplicar una transformació logarítmica.



3. **Premissa de Normalitat:**

Per utilitzar "t.test" cal que les diferències entre parelles ("Mètode-Mida") es distribueixin de forma aproximadament normal.
Primer comprovem si la $\mu_D$segueix una distribució normal. Si el QQ-plot mostra que els punts no segueixen la línia de regressió, no podrem aplicar el "t.test" directament sinó que haurem de transformar (aplicar logaritme) a les dades prèviament.
Com hem comentat anteriorment, a mesura que incrementi la mida, hauria d'incrementar el temps, però en fer el QQ-Plot no veiem de forma clara que no segueixi un model normal, cosa que és atípica.
Donat que anteriorment hem vist que estem davant un efecte multiplicatiu, definitivament haurem d'**aplicar** una **transformació logarítmica** a les dades per analitzar-ho.





Observem que:

- En el Q-Q Plot **previ** a **transformar** les **dades** podem observar una **forma** de "**S**" indicant que els quantils **no segueixen** prou bé la línia de regressió lineal **normal**.
- En el Q-Q Plot **posterior** a **transformar** les **dades** entre els **quantils** -1 i 1, els quantils de la diferència de mitjanes s'**aproximen** molt més als quantils teòrics d'una **normal**.

Intervals de Confiança.

Amb les mostres transformades sí que complim les premisses, és per això que podem realitzar un "t.test" de forma aparellada per determinar si la diferència de mitjanes és un fet "real" o casualitat.

```
Unset
       Paired t-test

data:  log(dades_parellades$`RSA-256`) and log(dades_parellades$`AES-256`)
t = 157.77, df = 24, p-value < 2.2e-16
alternative hypothesis: true mean difference is not equal to 0
95 percent confidence interval:
 3.692480 3.790367
sample estimates:
mean difference
       3.741424
```

D’aquest resultat podem treure els següents fets:

- El valor de “**t”** és molt gran, això implica que les **diferències observades** entre les dues mostres són molt **consistents** i no es poden atribuir a l’atzar.
- Com que el “**p.value**” és molt **petit**, és **molt poc probable** que les **dades** respecte a la **mitjana** i l’**IC** siguin **casualitat**.
- Donat que l’**interval de confiança no inclou** al **0** i és **positiu**, podem concloure que el **mètode** de ***RSA-256*** és **més costos en temps.**

```
Unset
Mitjana del factor multiplicatiu (RSA/AES): 42.15797
IC(95%) del factor multiplicatiu: 40.1443 44.27264
```

Si tornem a transformar els resultats mitjançant l’exponencial, podrem dir amb més seguretat que:

- De **mitjana** *RSA-256* és **42.15 vegades més lent** que *AES-256*. Donat que estem davant un efecte multiplicatiu.
- Amb una **confiança** del **95%** afirmem que *RSA-256* serà entre un **40.14 i 44.27 més lent** que *AES-256*.

Resultats

Mètode P	Mida M	Mitjana (MB)	Desviació Típica (seg.)
AES-256	1	0.00282	0.000146
AES-256	2	0.00562	0.00022
AES-256	3	0.00891	0.00101
AES-256	4	0.0149	0.00067
AES-256	5	0.018	0.00241
AES-256	6	0.0228	0.000668
AES-256	7	0.0281	0.00353
AES-256	8	0.0303	0.000758
AES-256	9	0.0345	0.00157
AES-256	10	0.0379	0.00131
AES-256	11	0.041	0.000859
AES-256	12	0.0456	0.0016
AES-256	13	0.0474	0.00155
AES-256	14	0.0537	0.00191
AES-256	15	0.0575	0.00204
AES-256	16	0.0606	0.00188
AES-256	17	0.0634	0.00184
AES-256	18	0.0672	0.00129
AES-256	19	0.0723	0.00412
AES-256	20	0.0836	0.00296
AES-256	21	0.089	0.00303
AES-256	22	0.0935	0.00236
AES-256	23	0.0982	0.00284
AES-256	24	0.101	0.000927
AES-256	25	0.107	0.00367

Mètode P	Mida M	Mitjana (MB)	Desviació Típica (seg.)
RSA-256	1	0.161	0.00943
RSA-256	2	0.312	0.00228
RSA-256	3	0.478	0.0129
RSA-256	4	0.629	0.00442
RSA-256	5	0.79	0.00497
RSA-256	6	0.948	0.00375
RSA-256	7	1.14	0.0358
RSA-256	8	1.28	0.0241
RSA-256	9	1.42	0.0166
RSA-256	10	1.62	0.0317
RSA-256	11	1.75	0.019
RSA-256	12	1.89	0.00625
RSA-256	13	2.05	0.0265
RSA-256	14	2.24	0.0127
RSA-256	15	2.41	0.0405
RSA-256	16	2.52	0.037
RSA-256	17	2.66	0.0128
RSA-256	18	2.86	0.031
RSA-256	19	3	0.0447
RSA-256	20	3.14	0.0333
RSA-256	21	3.27	0.0106
RSA-256	22	3.44	0.0171
RSA-256	23	3.58	0.0168
RSA-256	24	3.74	0.0315
RSA-256	25	3.98	0.0638

Anàlisis i Discussió

Els resultats obtinguts demostren que es rebutja la hipòtesi d'igualtat d'eficiència entre *AES-256* i *RSA-256*. Amb un interval de confiança del 95%, ***RSA-256* requereix** entre un **40%** i un **44% més de temps** que AES-256 per encriptar arxius.

La transformació logarítmica ha sigut necessària per complir les premisses de normalitat a causa de l'efecte multiplicatiu observat, on el temps d'encriptació augmenta exponencialment amb la mida dels fitxers.

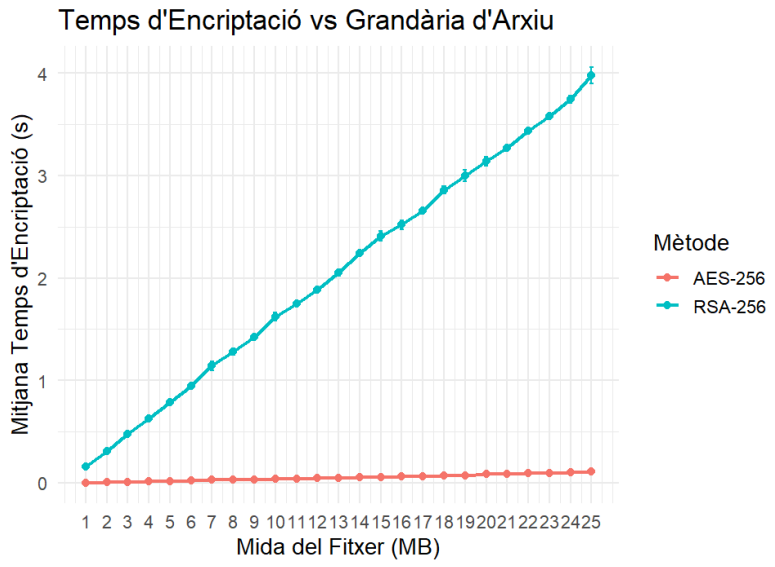
L'anàlisi estadística, mitjançant un "t-test" aparellat sobre dades log-transformades, confirma que aquesta **diferència no** és per **casualitat**.

En **mitjana**, ***AES-256*** és **42 vegades més eficient** que *RSA-256*.
Els intervals de confiança confirmen que RSA-256 és significativament més lent donat que no s'inclou el 0 i els extrems són positius (RSA - AES).

Gràfics de Suport

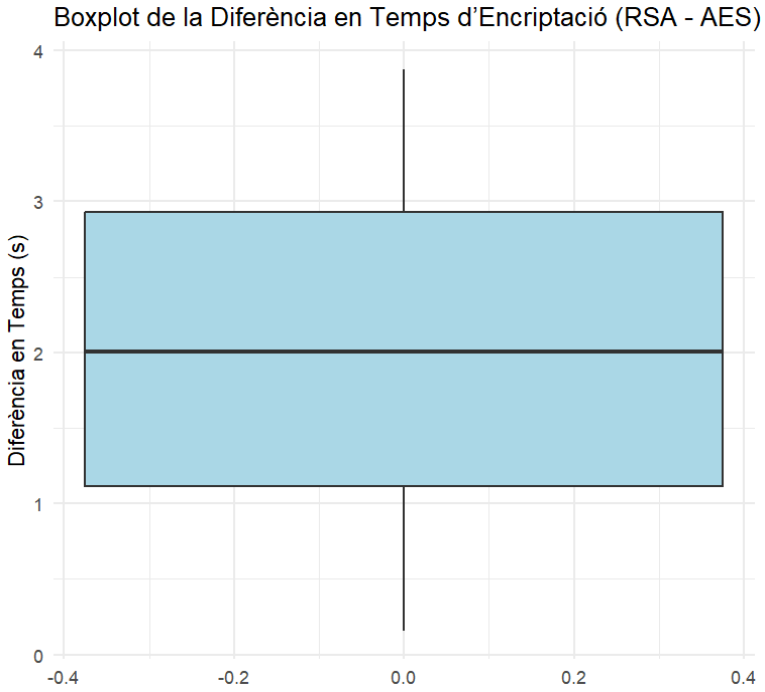
Gràfic 1: Temps d'Encriptació vs. Grandària d'Arxiu

El següent gràfic compara dos mètodes d'encriptació, AES-256 I RSA-256, en funció del temps que triguen a encriptar arxius de mides diferents.
Es pot observar que la magnitud del creixement exponencial del mètode RSA-256 és molt més elevat que el de AES-256.



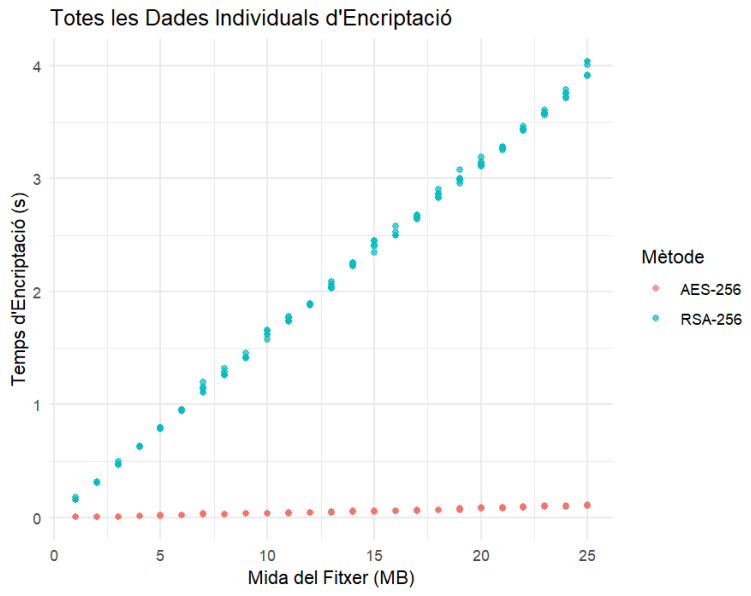
Gràfic 2: Boxplot del Temps d'Encriptació de la diferència

Aquest gràfic resumeix la distribució de les diferències individuals (RSA - AES). Es veu que la mediana de la diferència és clarament superior a zero i la majoria dels valors se situen per sobre de zero, indicant que RSA-256 triga més que AES-256 de forma consistent.



Gràfic 3: Scatter Plot de Totes les Dades Individuals

Aquest nou gràfic mostra tots els punts individuals de temps d'encriptació per a cada mida, diferenciant AES-256 i RSA-256 amb colors. Permet veure la variabilitat interna i com, per a cada mida, els valors d'RSA són sistemàticament més alts. A mesura que la mida creix, els punts d'RSA s'allunyen molt més dels d'AES.



Recomanacions

Basat en els resultats obtinguts, es recomana:

1. **Ús d'AES-256 per a encriptació de fitxers grans**: Donada la seva eficiència en termes de temps, AES-256 hauria de ser l'opció preferida per a aplicacions que gestionen grans volums de dades.

2. **Ús de RSA-256 per a encriptació de fitxers petits**: Per a fitxers de mida petita, la diferència en temps pot ser menys significativa. És per això que, com a experts en informàtica, recomanem fer ús de RSA-256 per a fitxers petits, com claus, donada la seva robustesa i seguretat donat que el temps emprat és gestionable.

Annex

Informació de l'ordinador

Ítem	Valor
Sistema Operatiu	Ubuntu 22.04.5 LTS
Processador	AMD Ryzen 7 2700 Eight-Core Processor, 3200 Mhz, 8 Core(s), 16 Logical Processor(s)
RAM	16.0 GB

Versions de programes

Ítem	Valor
g++	Ubuntu 11.4.0
OpenSSL	3.4.0
Chrono	9.0.1
R	4.4.2
RStudio	2024.09.0

Enllaços Generals

- Dades (CSV) de l'estudi

https://github.com/impulsado/EternalFIB/blob/main/PE/BT/dades.csv

- Codi del programa (C++) per generar fitxers, encriptar-los i mesurar el temps.

https://github.com/impulsado/EternalFIB/blob/main/PE/BT/encriptar.cpp

- Codi del script (R) per analitzar les dades obtingudes

https://github.com/impulsado/EternalFIB/blob/main/PE/BT/script.R