

Segurança e Privacidade

Mestrado em Engenharia e Ciência de Dados

2022/2023

Assignment 1:

Data Sharing with Encryption

Duarte Emanuel Ramos Meneses – 2019216949 – duartemeneses@student.dei.uc.pt

Patrícia Beatriz Silva Costa – 2019213995 – patriciacosta@student.dei.uc.pt

Índice

[Introdução 3](#_Toc116388322)

[1. Modelo de ameaça: quem são os invasores e quais são as suas capacidades 4](#_Toc116388323)

[2. Desenho do esquema de comunicação 4](#_Toc116388324)

[2.1. Sem validação da Autenticidade e Integridade 4](#_Toc116388325)

[2.2. Com validação da Autenticidade e Integridade 4](#_Toc116388326)

[5. Análise de dados 5](#_Toc116388327)

[5.1. Impacto das colunas ‘past’ nos incumprimentos 5](#_Toc116388328)

[5.2. Impacto da idade dos clientes nos empréstimos em incumprimento 6](#_Toc116388329)

[6. Tempo de execução 6](#_Toc116388330)

[Conclusão 6](#_Toc116388331)

[Referências 6](#_Toc116388332)

# Introdução

Nos dias que correm, o mundo é controlado por informação (dados). Como tal, para que não aconteça nenhuma desgraça na sociedade, é necessária a presença de segurança nas trocas de informação.

É com isso em vista que este trabalho prático procura simular a troca de informações confidenciais entre duas empresas. Para tal, são utilizados mecanismos de troca de chaves e de encriptação/desencriptação.

Ao longo deste relatório vamos abordar o modelo de ameaça ao sistema, o esquema de comunicação e vamos analisar brevemente dados relativos a empréstimos em incumprimento, bem como o tempo de execução do nosso programa com e sem mecanismos de validação da autenticidade e da integridade.

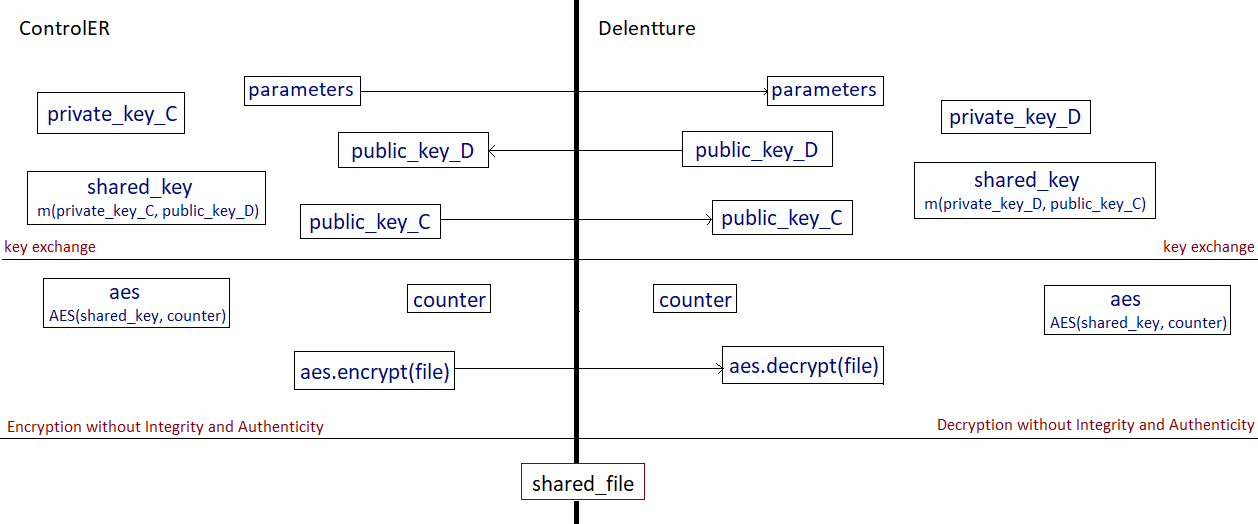
# 1. Modelo de ameaça: quem são os invasores e quais são as suas capacidades

A troca de informação entre a ControlER e a Delentture acarreta muitos riscos de segurança e privacidade. Um intruso pode colocar-se no meio da comunicação e intersetar ficheiros confidenciais.

O atacante pode ainda aceder ao sistema de ficheiros de uma máquina (ou mesmo à máquina em si), tendo acesso a ficheiros que não devia.

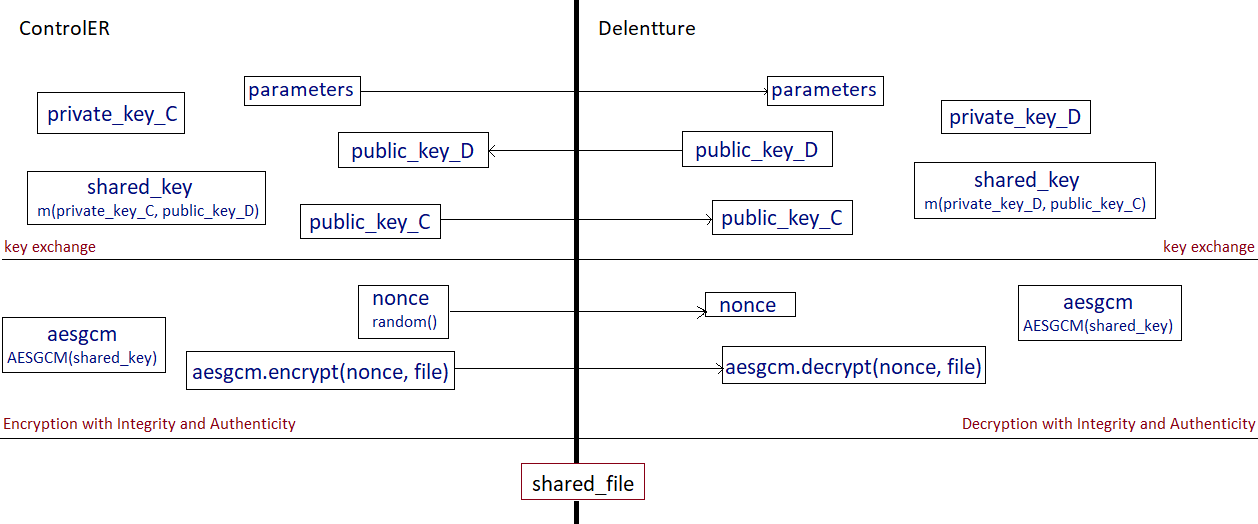
# 2. Desenho do esquema de comunicação

## 2.1. Sem validação da Autenticidade e Integridade

Decidimos utilizar o algoritmo de Diffie-Hellman para trocar a chave e o AES em modo CTR para encriptar o ficheiro.

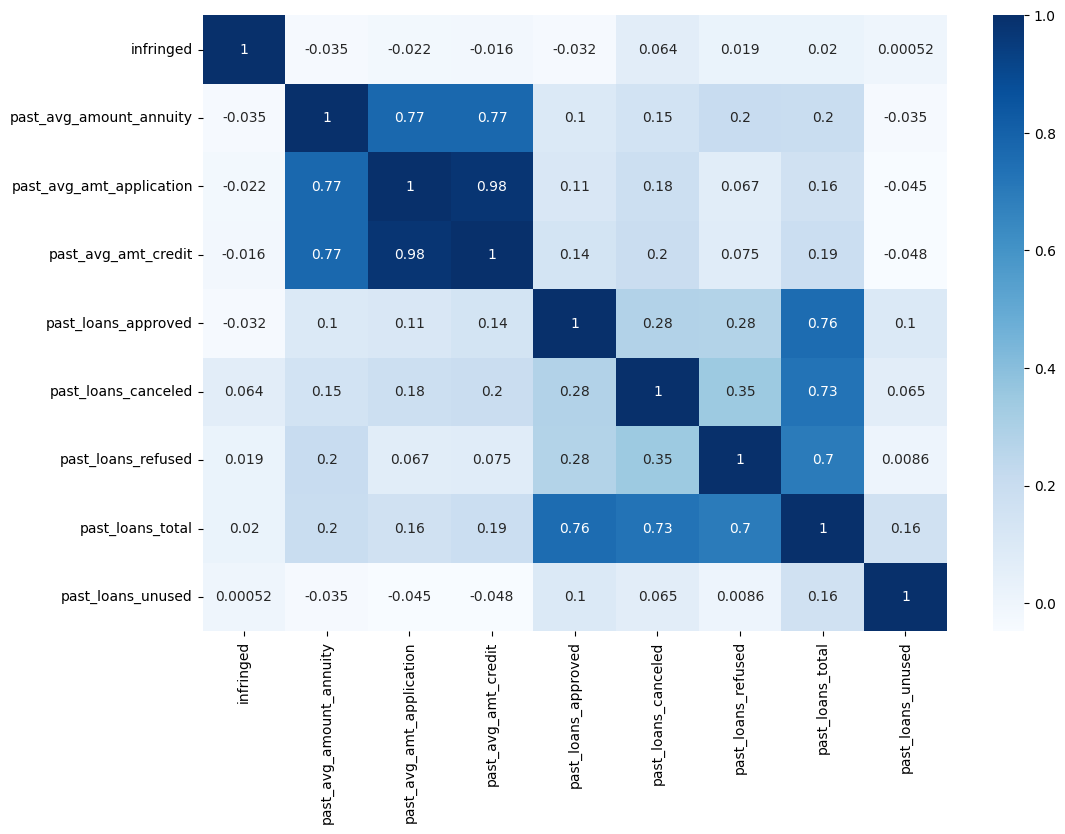
## 

## 2.2. Com validação da Autenticidade e Integridade

Já neste caso, optámos por utilizar o algoritmo de Diffie-Hellman para trocar a chave e o AESGCM para encriptar o ficheiro.

# 5. Análise de dados

## 5.1. Impacto das colunas ‘past’ nos incumprimentos

Decidimos visualizar o impacto das colunas ‘past’ com os empréstimos não cumpridos através da correlação entre essas colunas. O resultado é o seguinte:

Fica claro que a coluna ‘past’ que mais impacto tem nos empréstimos em incumprimento é a coluna dos empréstimos passados cancelados. Podemos deduzir que estes foram cancelados precisamente por estarem em incumprimento.

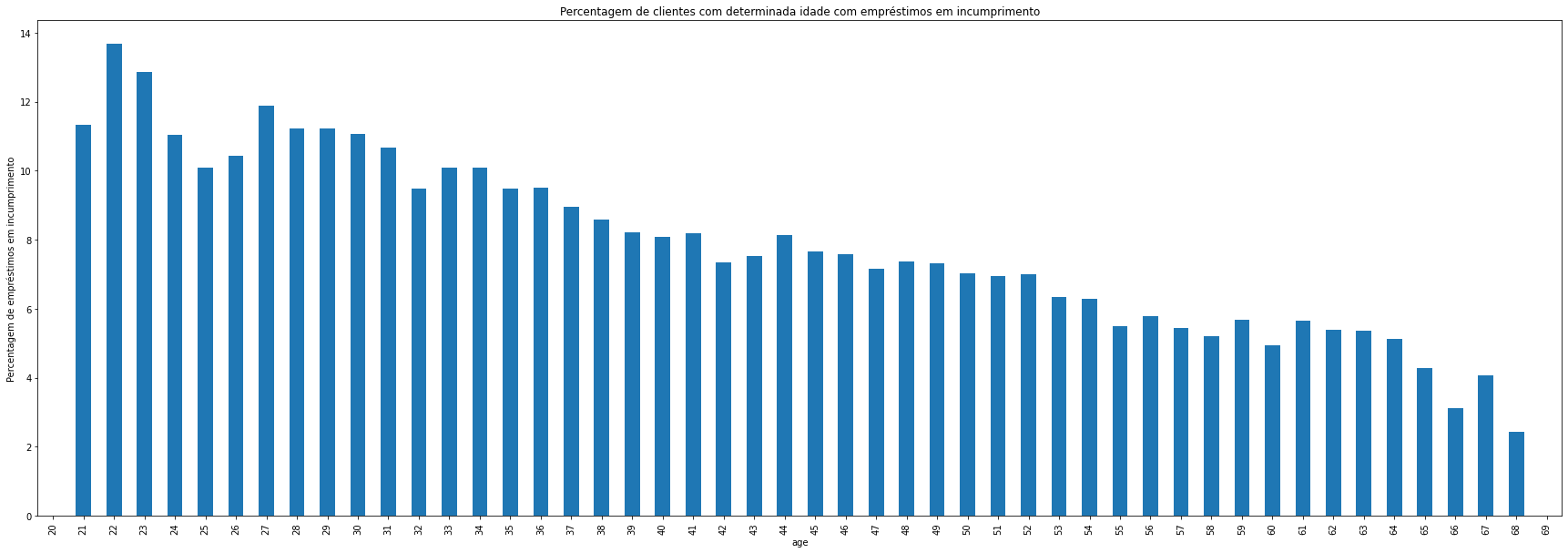
Embora com impacto inferior, as colunas relativas a empréstimos passados recusados e totais também têm alguma correlação com os em incumprimento. Podemos explicar isto uma vez que, talvez os empréstimos tenham sido recusados por, no passado, o cliente ter alguns em incumprimento e, quanto ao número total, quantos mais empréstimos um cliente tem, mais provável é a existência de incumprimentos.

Por último, com ainda menos impacto, a coluna que diz respeito aos empréstimos aprovados mas não utilizados pelo cliente tem uma ligeira correlação com a coluna dos em incumprimento. Isto pode-se explicar já que o cliente pode não utilizar um empréstimo aprovado pois tem outros já em incumprimento.

Nenhuma outra coluna ‘past’ tem impacto na coluna ‘infringed’.

## 5.2. Impacto da idade dos clientes nos empréstimos em incumprimento

Nesta secção, decidimos analisar o impacto da idade dos clientes nos empréstimos em incumprimento. Para tal, analisamos a percentagem de pessoas com determinada idade com empréstimos em não cumprimento. Os resultados foram os seguintes:



Tal como era espectável, quanto mais novos são os clientes, a percentagem de empréstimos em incumprimento é superior. Podemos explicar isto, uma vez que com a idade vai-se ganhando estabilidade financeira. Posto isto, quanto mais velho for um cliente, teoricamente, mais capacidades tem de pagar um empréstimo.

# 6. Tempo de execução

Para esta questão, decidimos realizar cinco medições de tempo para cada caso para evitar possíveis *outliers*. As medições podem ser consultadas em detalhe no anexo “Tempos.csv”. Os resultados finais obtidos foram os seguintes (sendo Mx referente á medição número x):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Troca de chave + Encriptação sem validação da Autenticidade e Integridade | | | | | |
| Tempos | M1 | M2 | M3 | M4 | M5 |
| 3,345 | 3,436 | 4,669 | 3,856 | 3,012 |
| Média | 3,6636 | | | | |
| Desvio Padrão | 0,570217 | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Troca de chave + Encriptação com validação da Autenticidade e Integridade | | | | | |
| Tempos | M1 | M2 | M3 | M4 | M5 |
| 3,413 | 3,312 | 3,306 | 4,485 | 3,123 |
| Média | 3,5278 | | | | |
| Desvio Padrão | 0,487655 | | | | |

Analisando os resultados acima, percebemos que na medição dos tempos do algoritmo com validação da autenticidade e integridade existiram menos outliers que no outro caso. No entanto, isso não é relevante, uma vez que o desvio padrão, apesar de o comprovar, não tem um valor muito significativo.

Tendo medido cinco vezes em cada caso, consideramos que a média obtida espelha bem a duração de cada algoritmo.

À priori, esperávamos que um algoritmo que tenha mecanismos de validação da integridade e autenticidade demorasse mais tempo visto ter de efetuar mais operações, o que leva a que demore mais tempo. Aliado a isto, o AES\_CTR aplica encriptação em blocos paralelamente, o que acelera o processo, tornando-o mais rápido.

No entanto, não é isso que os resultados demonstram.

# Conclusão

# Referências