Trabalho Prático 01

Tema B
Encriptação/Desencriptação

João Neves 240001565

Tomás Marques 210100063

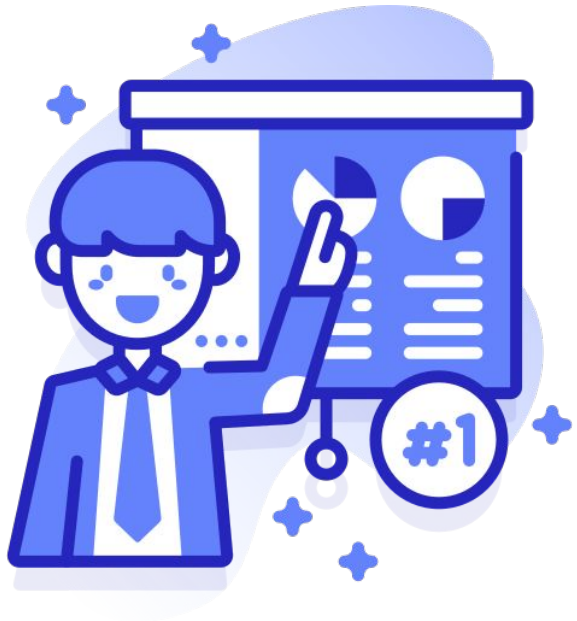
Tecnologias de Segurança - MIA

POLITÉCNICO DE SANTARÉM

Índice - Tema e Apresentação

Estrutura da apresentação

- Proposta e objetivos do trabalho;
- Conceitos de estudo;
- Arquitetura da implementação;
- Demonstração ao vivo;
- Possíveis melhorias;
- Fragilidades;
- Conclusão;



Objetivo e proposta do trabalho - Tema B

Implementação de algoritmo(s) de encriptação/desencriptação

- Entender o conceito de encriptação;
- Entender o conceito de desencriptação;
- Criar um Algoritmo Robusto;
- Alcançar 100% de fator de confiança;
- Procurar dificultar a intercepção e obtenção da mensagem original;

Conceitos de estudo - Parte 1

Encriptação

- Transformar informação, com recurso a um algoritmo, de forma a que apenas quem o consiga decifrar e obter a mensagem original;

Desencriptação

- Utilizar o algoritmo que foi utilizado na encriptação de forma a obter a mensagem original;

Salt

- Dados aleatórios adicionados à mensagem para serem usados no processo de encriptação;

Fator de confiança

- Qualidade da desencriptação;
- Se com a mesma mensagem e mesmo algoritmo, conseguimos sempre obter a mensagem original, sem depender de fatores externos;

Conceitos de estudo - Parte 2

Chaves Simétricas

- Utilizadas tanto para encriptar como para desencriptar
  Ex: AES;

Chaves Assimétricas

- Par de chaves, uma para encriptar e outra (relacionada de alguma forma com a primeira) para desencriptar
  Ex: RSA;

Hashing

- Transformar dados numa sequência de caracteres de tamanho fixo;
- Diferentes dados podem produzir a mesma hash, impedindo a desencriptação de forma direta;

Entropia

- “Quantidade” de aleatoriedade de uma chave ou senha;

Conceitos de estudo - Parte 3

Nonce

- Número aleatório utilizado apenas uma vez, que garante que a mesma chave e dados não resultem sempre da mesma encriptação;

AES-GCM

- Extensão de AES que adiciona um Nonce concatenado com os dados encriptados e um Checksum para validar a integridade dos dados

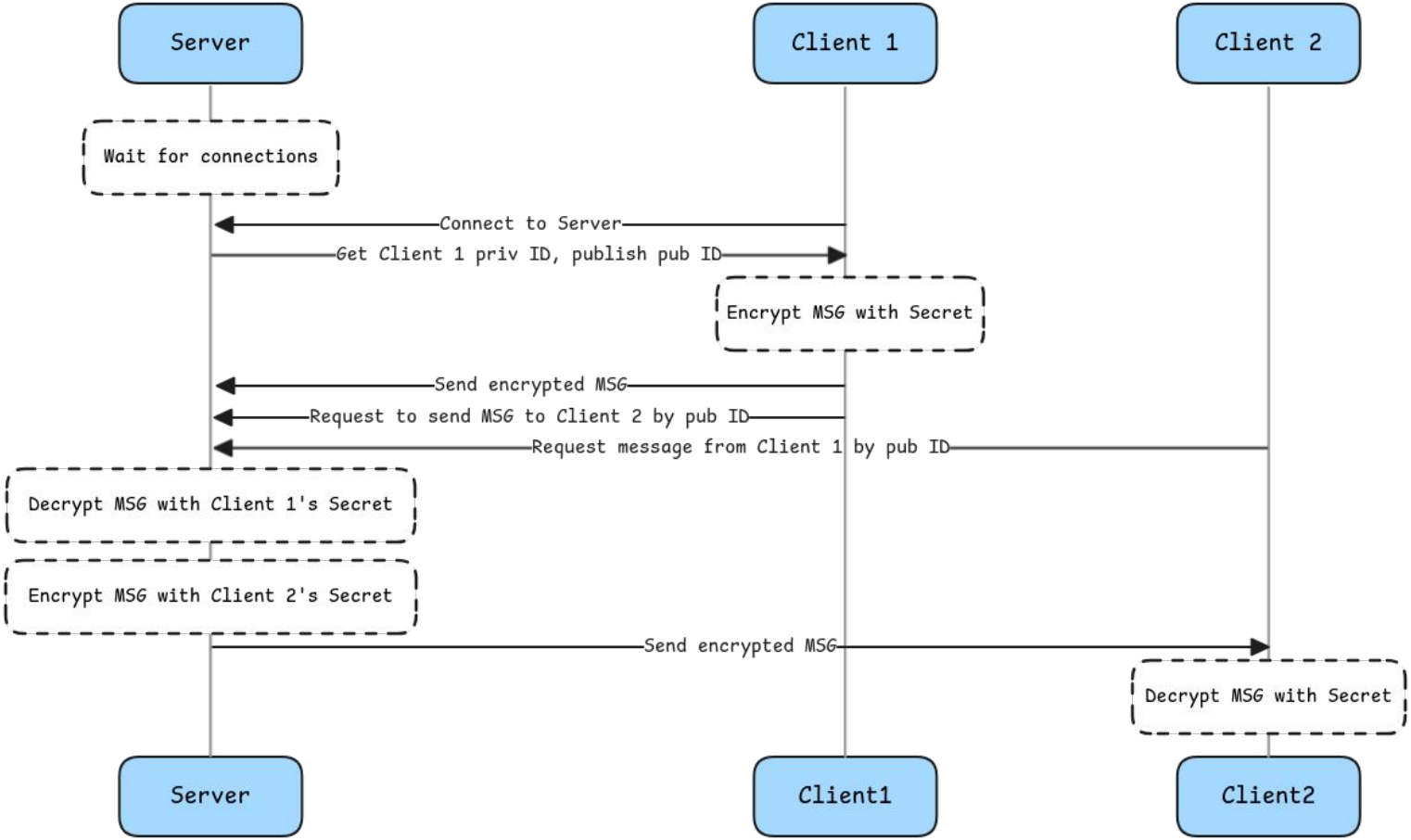
Checksum

- Normalmente um dígito resultante de uma operação nos dados;
- Serve para garantir a integração dos mesmos;
- Utilizado por exemplo no Cartão de Cidadão;

Secret

- Chave criptográfica derivada de dados aleatórios;

Implementação - Arquitetura



DEMO

Encriptação - Intercepção - Desencriptação

Possíveis Melhorias

HTTPS

- Um *web server* HTTPS melhoraria a segurança da transmissão da mensagem encriptada, acrescentando outra camada de proteção;

Chaves assimétricas

- A utilização de um par de chaves (uma pública e uma privada) poderia ajudar a melhorar a segurança da transmissão da mensagem;

Secret de tamanho variável

- A variação no tamanho do *secret* acrescentaria ainda mais entropia à encriptação, dificultando ataques;

Interface Gráfica

- Poderia tornar a utilização do cliente mais intuitiva e apelativa ao consumidor final;

Fragilidades - e falta delas...

Brute Force ❌

- Seria virtualmente impossível a desencriptação por brute force em tempo útil devido ao elevado nível de entropia da encriptação utilizada;

Replay Attacks ❌

- A utilização de Nonce inviabiliza este tipo de ataque, já que para o mesmo input podem existir diferentes outputs, dificultando associações entre mensagens;

Timing Attacks ➕/➖

- Apesar de ser possível retirar algumas conclusões através do estudo dos tempos de execução de cada passo, muito dificilmente levaria a alguma informação útil e vital para a desencriptação;

Side-Channel Attacks ➕/➖

- A utilização de hardware inseguro pode comprometer a segurança da mensagem;

Referências e Bibliografia

Vulnerability Types | *https://security.snyk.io/package/pip/cryptography*

Cryptography Techniques | *https://www.simplilearn.com/cryptography-techniques-article*