Trabalho 2 Segurança de Sistemas

Jeniffer Moreira Borges,Enzo Contursi Silveira

1

Abstract. *This project aims to demonstrate a simulation of a comunication that uses HTTPS protocol with Diffie-Hellman cypher*

Resumo. *Este trabalho tem o intuito de demonstrar como foi feita uma simulação de troca de mensagens do protocolo HTTPS utilizando a cifra de Diffie-Hellman*
Keywords: Diffie-Hellman, HTTPS, CBC, AES.

1. Introdução

A cifra de Diffie-Hellman é um método criptográfico que consiste em uma troca de chaves para comunicação em um canal inseguro. Para garantir sua segurança contra ataques de força bruta, utiliza-se a dificuldade do problema do logaritmo discreto. O processo começa com a escolha de um número primo p e um gerador g, ambos de conhecimento público. Cada parte escolhe um valor secreto, a e b, e realiza os seguintes cálculos:

- $A = g^a p$
- $B = g^b p$

Esses valores, A e B, são então trocados entre as partes. Com os valores recebidos, cada parte pode calcular a chave compartilhada V:

- $V = B^a p$
- $V = A^b p$

Como $B^a p = A^b p$, ambas as partes têm o mesmo V, que é utilizado como chave para comunicação segura. A dificuldade de calcular a ou b a partir de A ou B, devido ao logaritmo discreto, é o que protege o processo contra interceptação.

2. Problema a ser resolvido

O problema proposto consiste em implementar uma simulação do protocolo HTTPS dividida em duas etapas:

- 1 Geração de uma chave utilizando a troca de chaves Diffie-Hellman;
- 2 Comunicação de mensagens cifradas utilizando o algoritmo AES no modo CBC.

Na **Etapa 1**, cada parte deve:

- Escolher um valor secreto a maior que 30 dígitos e calcular o valor público $A = g^a p$.
- Receber um valor público B, fornecido pelo professor, e utilizá-lo para calcular a chave compartilhada $V = B^a p$.
- Derivar a chave de sessão S a partir de V utilizando os 128 bits menos significativos do hash SHA-256 de V.

Na **Etapa 2**, a comunicação é realizada através de mensagens cifradas no formato:

- $[128bitsdoIV][mensagemcifrada]$.

A mensagem deve ser decifrada utilizando o AES-CBC com a chave de sessão S. Após isso, a resposta à mensagem deve:

- Conter a mesma mensagem, mas com os caracteres invertidos.
- Ser cifrada novamente com um IV aleatório e enviada no formato $[128bitsdonovoIV][mensagemcifrada]$.

Essas etapas simulam elementos fundamentais do protocolo HTTPS, garantindo a troca segura de informações entre duas partes. A implementação deve respeitar os requisitos de segurança e formatação definidos no enunciado, como a utilização de padding nos blocos e a geração de valores aleatórios para o vetor de inicialização.

3. Resolução do problema

3.1. Atividade 1

Com os valores p e g já fornecidos foram utilizadas as seguintes bibliotecas para a geração das chaves necessárias para a cifra de Diffie-Hellman

- **random**: Para gerar a chave privada a como um número aleatório grande dentro de um intervalo de 10^{29} e $p - 1$.
- **pow** : Para cálculo de potências modulares, utilizados na geração da chave pública A.
- **hashlib**: Para derivar a chave de sessão S através da função hash SHA-256.

Os valores gerados foram:
a **(chave privada):**

```
0xd559f3f776c7ccd8b38b31d83e1c82cc64fd63c338ce71b7e00cf13d92f1606d
f1d947efc08a2116850c052c708ae5644f399fc20d2618d94a7b50b629a63565
6a741bc2c7b55915dc08efff9b18ad09fba19e1667c7699069082761f092e100
431f2a57eee0b2364b2d38fc5d5dfd9c496e9ec67129d706d422ceec47819a3
```

A **(chave pública):**

```
0x2e2239b714154af689aa06a976d5a9b926259718d5d6512b777e09dcbe9661d
deed64457c386f9c12f9e6179b35c5bde61967f538659fc5ce586aa1bae0629c
7fe55be69e06ec8f2dcb1385ed1f01acd69c5c7c56173fa107c3da6d033630bb
17f031e96d05792020d1655a1048f4d28e96c0b509d14b8b3f82b80afe91ac43d
```

Chave de sessão S**:**

```
7909760995592414cd21a71b2892cb40
```

Valor de V**:**

```
51191775297603079376584466993263844869064882704998389191875927133175067066432455407820467948587883145854464387396124471274598905593165669147031038695926612150898264636841987903108391566120074458898280877340680303118059453852794111949218432847615974634268740003387890726583165200101630049854055016854096866560
```

A chave pública A foi postada no moodle para obtermos a chave pública do professor junto de uma mensagem criptografada

3.2. Atividade 2

Para decifrar a mensagem, invertê-la e depois cifrá-la novamente foram usadas as seguintes bibliotecas do python

- **cryptography**: Para cifrar e decifrar mensagens utilizando o AES no modo CBC.
- **hashlib**: Para manipulação de hashes e derivação da chave de sessão S.
- **secrets**: Para a geração de vetores de inicialização (IVs) aleatórios.

Foi seguido esse fluxo para a resolução dessa etapa

1. Receber a mensagem cifrada no formato $[128bitsdoIV][mensagemcifrada]$, onde o IV (vetor de inicialização) é necessário para a decifração.
2. Utilizar a chave de sessão S para inicializar o algoritmo AES em modo CBC.
3. Decifrar a mensagem utilizando o módulo `Cipher` da biblioteca `cryptography`.
4. Remover o padding (preenchimento) da mensagem decifrada para obter o texto claro.
5. Processar a mensagem decifrada, invertendo seus caracteres para produzir a resposta.
6. Gerar um novo IV aleatório para cifrar a resposta.
7. Cifrar a mensagem invertida utilizando o mesmo algoritmo AES em modo CBC.
8. Enviar a resposta cifrada no formato $[128bitsdonovoIV][mensagemcifrada]$.

Por fim estes foram os valores encontrados:

Mensagem decifrada (bytes):

```
4d41495320554d204d455320452041532046455524
94153204553434f4c4152455320434f4d4543414d
```

Mensagem decifrada:

MAIS UM MES E AS FERIAS ESCOLARES COMECAM

Resposta cifrada:

```
84719f97eb8da83b8c7f158107926b7a02477049e562948d081a7bb52fd91cb77848f
c50696ea2eed7458d38355ea1d534f222e0fdf97ae412987d12c5c2aed2
```

Resposta - Mensagem invertida (bytes):

```
4d4143454d4f4320534552414c4f435345205341495
24546205341204520534 54d204d5205349414d
```

Resposta - Mensagem invertida:

MACEMOC SERALOCSE SAIREF SA E SEM MU SIAM

4. Considerações Finais

Este trabalho foi de grande importância para aprofundar os conhecimentos sobre criptografia, permitindo uma compreensão mais prática dos processos de cifrar e decifrar informações de maneira segura. A experiência proporcionou uma visão mais clara sobre os algoritmos como Diffie-Hellman e AES-CBC, além de demonstrar mais sobre como é trabalhar com codificação de dados e troca de chaves em sistemas. Um dos maiores desafios enfrentados foi identificar corretamente a codificação do texto recebido, que estava em Latin1. Esse problema foi solucionado apenas após a terceira sequência de chaves fornecida pelo professor no Moodle.

Referências

Stinson, D. R. (2006). *Cryptography: Theory and Practice*. CRC Press.

[Stinson 2006]