Segurança de Sistemas/Criptografia – Simular HTTPS

Prof. Avelino Zorzo – Escola Politécnica /PUCRS

Este trabalho tem como objetivo simular parte do funcionamento do HTTPS.

Para o trabalho considere os valores de número primo p e gerador g abaixo (RFC5114):

```
p = B10B8F96 A080E01D DE92DE5E AE5D54EC 52C99FBC FB06A3C6
    9A6A9DCA 52D23B61 6073E286 75A23D18 9838EF1E 2EE652C0
    13ECB4AE A9061123 24975C3C D49B83BF ACCBDD7D 90C4BD70
    98488E9C 219A7372 4EFFD6FA E5644738 FAA31A4F F55BCCC0
    A151AF5F 0DC8B4BD 45BF37DF 365C1A65 E68CFDA7 6D4DA708
    DF1FB2BC 2E4A4371

g = A4D1CBD5 C3FD3412 6765A442 EFB99905 F8104DD2 58AC507F
    D6406CFF 14266D31 266FEA1E 5C41564B 777E690F 5504F213
    160217B4 B01B886A 5E91547F 9E2749F4 D7FBD7D3 B9A92EE1
    909D0D22 63F80A76 A6A24C08 7A091F53 1DBF0A01 69B6A28A
    D662A4D1 8E73AFA3 2D779D59 18D08BC8 858F4DCE F97C2A24
    855E6EEB 22B3B2E5
```

O trabalho é dividido em 2 etapas:

Etapa 1: Geração de chave usando Diffie-Hellman:

Passo 1: gerar um valor **a** menor que **p** (dado) e calcular $A = g^a \bmod p$. Enviar o valor de A (em hexadecimal) para o professor.

Passo 2: receber um valor B (em hexadecimal) do professor e calcular $V = B^a \bmod p$

Passo 3: calcular S = SHA256(V) e usar os primeiros 128 bits como senha para se comunicar com o professor.

Etapa 2: Troca de mensagens

Receber uma mensagem do professor (em hexadecimal), cifrada com o AES no modo de operação CBC, e padding. Formato da mensagem recebida: [128 bits com IV][mensagem] – em hexadecimal.

Decifrar a mensagem e mandar ela de volta ao professor cifrada e invertida (em hexadecimal), ou seja, se receber "ola", mandar de volta "alo". Formato da mensagem a ser enviada: [128 bits com IV aleatório][mensagem] – em hexadecimal.

Fazer um programa que:

Para a Etapa 1, recebe um valor hexadecimal (valor B) e imprime A em hexadecimal e os 128 primeiros bits de S em hexadecimal.

Para a Etapa 2, recebe a mensagem e a chave (128 primeiros bits de S em hexadecimal), e imprime a mensagem recebida (em texto claro) e a mensagem a ser enviada (em hexadecimal).

Entrega: programa comentado com os valores enviados/gerados/recebidos. As mensagens podem/devem ser enviadas antes.