Segurança de Sistemas

Trabalho Prático 2 – Simulador de HTTPS

O presente trabalho tem por objetivo explorar parte dos assuntos abordados em sala de aula. Neste contexto, deverá ser desenvolvida uma solução que simula parte do protocolo HTTPS.

Para o desenvolvimento deste trabalho, são compartilhados dois valores, correspondente ao número primo *p* e o número gerador, conforme segue:

```
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
```

Atividade a ser desenvolvida

O trabalho a ser desenvolvido compreende duas etapas: (a) Geração/Definição da chave usando Diffie Hellman e (b) a troca de mensagens de forma segura.

Atividade 1 – Geração da chave

Cada grupo deve gerar um valor *a* menor que *p*. Apesar de ser um valor menor, *a* não deve ter menos do que 30 dígitos. A partir desta definição, o grupo deve calcular $A = g^a \bmod p$. O valor definido para A deve ser enviado para que o professor via moodle. O valor de A deve ser informado em base hexadecimal.

Com base no valor gerado o professor gerará um valor B que será divulgado no moodle. O valor B informado deverá ser então utilizado pelos alunos para calcular $V = B^a \bmod p$

Por fim, cada grupo deverá calcular S = SHA256(V) e usar os 128 bits menos significativos (menores) como senha para se comunicar com o professor. Usar os bytes de V para gerar S. Esta será a chave da seção.

Atividade 2 – Troca de mensagem de forma segura

Será enviada/disponibilizada uma mensagem do professor, cifrada com o AES no modo de operação CBC, e *padding*. O formato da mensagem será recebida: [128 bits com IV][mensagem]. Toda informação estará em um bloco de dígitos em hexadecimal.

O grupo deverá decifrar a mensagem e mandar ela de volta ao professor cifrada. O conteúdo da mensagem de resposta deve ser a própria mensagem, porém com seus caracteres invertidos, ou seja, se receber “ola”, mandar de volta “alo”. O formato da mensagem a ser retornada pelos alunos é: [128 bits com IV aleatório][mensagem]. Assim como a mensagem original enviada, toda a informação estará em um bloco de dígitos em hexadecimal.

A entrega do trabalho (local e artefatos)

O trabalho deve ser postado no moodle conforme detalhe na sala de entrega.

A condução da etapa 1 e da etapa 2 exige a troca de mensagens para sua realização. Para isso, deve-se utilizar o fórum do moodle para tanto. No fechamento deste trabalho, todo material gerado deve se encaminhado na sala de entrega do moodle.

Devem ser postado um arquivo zip contendo os fontes do projeto e um pequeno relatório conforme detalhado na seção que segue. Este arquivo zip deverá ser nomeado com o nome dos integrantes do grupo.

Reforçando o que é esperado, para a Etapa 1, deve-se desenvolver uma solução que gera um valor “a” e valor “A” (imprime estes dois valores em hexadecimal) ou recebe um valor hexadecimal (valor B) e “a” gerado anteriormente e imprime os 128 primeiros bits de S em hexadecimal. Já para a Etapa 2, deve-se desenvolver uma solução que receba uma 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).

Adicionalmente, o grupo deve fazer um vídeo de 5 a 10 minutos explicando como o trabalho foi desenvolvido. Este vídeo deve ser salvo no *youtube* e o link deve ser informado no relatório. Por questões de prazo de fechamento do semestre, não serão aceitas postagens posteriores ao momento especificado, não sendo permitido o envio por mail ou qualquer outra forma que não o uso do moodle.

Pontos que serão considerados na avaliação

Para o presente trabalho, serão avaliados os seguintes pontos.

- Soluções elaborada (6,0 ptos)
    - Solução elaborada para a etapa 1
    - Solução elaborada para a etapa 2
- Recursos adicionais na avaliação (4,0 ptos)
    - Relatório (3,0 pto)
        - Apresentação
            - Formatação
                - Capa, Capítulos, ...
                - Texto com alinhamento justificado
            - Organização
                - Frases curtas e objetivas
                - Encadeamento de ideias
                - Escrita coerente e adequada
        - Conteúdo
            - Detalhamento da solução
            - Detalhamento da implementação
            - Processo de compilação
    - Vídeo de apresentação (1,0 pto)

- Não exceder os 10 min
- Explicação de forma clara e objetiva

Considerações finais sobre o trabalho

Um ponto importante e que será considerado na avaliação é a presencialidade. Todos os membros de um grupo devem ter participação tanto na condução dos trabalhos quanto das apresentações (vídeo). Tanto no relatório quanto no vídeo, deve ficar clara a contribuição de cada um no desenvolvimento do trabalho.

Os itens a serem considerados na avaliação do trabalho foram listados anteriormente. Cabe ressaltar que os pontos listados servem de apoio tanto para o aluno entender como será avaliado quanto cria um roteiro de pontuação para o professor. Porém, algumas situações podem fazer com que os critérios adotados sejam postos de lado e a atribuição de notas zero sejam atribuídas independente do que for entregue. São estas situações:

1. Fraude acadêmica: O uso de recursos que não permitam ao professor avaliar o conhecimento empregado pelo aluno no desenvolvimento da solução. Exemplos de fraude acadêmica são, mas não se limitam a isto: (a) uso de ferramentas de geração de solução (tal como ChatGPT); (b) a cópia integral ou parcial do material entregável.
2. Não funcionamento da solução: caso não seja possível visualizar a solução elaborada, não faz sentido avaliar o trabalho. Toda solução entregue tem de ser compilável e executável.