Roteiro
Aula Prática

CRIPTOGRAFIA

ROTEIRO DE AULA PRÁTICA

NOME DA DISCIPLINA: CRIPTOGRAFIA

Unidade: INTRODUÇÃO À CRIPTOGRAFIA

Seção: Algoritmos de chaves assimétricas

OBJETIVOS

Definição dos objetivos da aula prática:

- Compreender os princípios da criptografia assimétrica e o funcionamento do algoritmo RSA.
- Aprender a gerar chaves pública e privada a partir de números primos.
- Realizar uma atividade prática complexa demonstrando a aplicação dos conceitos aprendidos.

INFRAESTRUTURA

Instalações – Materiais de consumo – Equipamentos:

LABORATÓRIO DE INFORMÁTICA

Equipamentos:

- Desktop Lab Informatica - Positivo C6300

~ 1 un por grupo de alunos

SOLUÇÃO DIGITAL

- IDLE(PYTHON) (Software)

IDLE(Python): É um ambiente de desenvolvimento integrado (IDE) para a linguagem de programação Python. Ele é usado principalmente para desenvolvimento de aplicativos em Python e inclui recursos como realce de sintaxe, depuração, controle de versão e muito mais.

EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL (EPI)

Não se aplica

PROCEDIMENTOS PRÁTICOS

Procedimento/Atividade nº 1 (Físico)

Atividade proposta:

Nesta atividade, você aplicará seus conhecimentos sobre criptografia RSA, chaves pública e privada, e geração de chaves a partir de números primos. Vamos criar um cenário em que você precisa enviar uma mensagem segura para um amigo, utilizando criptografia RSA.

Procedimentos para a realização da atividade:

Passo 1: Geração de Chaves

Gere dois números primos grandes, p e q.

Para isso, você pode usar ferramentas online, como calculadoras de números primos.

Certifique-se de que p e q sejam números primos diferentes e mantenha esses valores em segredo.

Passo 2: Cálculo de n e $\varphi(n)$

Calcule n = p * q e $\varphi(n) = (p-1)(q-1)$.

Mantenha esses valores em segredo.

Passo 3: Escolha da Chave Pública

Escolha um número e, em que $1 < e < \varphi(n)$, e que seja co-primo de $\varphi(n)$.

Isso será sua chave pública (n, e).

Passo 4: Cálculo da Chave Privada

Calcule d, que é o inverso multiplicativo de e (mod $\varphi(n)$). Ou seja, $d * e = 1 \pmod{\varphi(n)}$.

d será a sua chave privada.

Passo 5: Mensagem e Criptografia

Escolha uma mensagem M que você deseja enviar e converta-a em um número inteiro M.

Certifique-se de que M seja menor que n.

Criptografe a mensagem M utilizando a chave pública (n, e) e a fórmula: C = M^e (mod n).

O resultado, C, será a mensagem criptografada.

Passo 6: Descriptografia e Mensagem Decifrada

Envie C para o seu amigo.

Seu amigo deve possuir a chave privada (d) para descriptografar a mensagem. Para isso, ele usará a fórmula: M = C^d (mod n).

Sugestão de aplicação:

Para realizar essa atividade você pode usar a linguagem de programação Python e a biblioteca criptográfica "cryptography".

```python
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes

# Geração de chaves
private_key = rsa.generate_private_key(public_exponent=65537, key_size=2048

# Conversão das chaves em formato PEM
private_pem = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)

# Geração da chave pública
public_key = private_key.public_key()
public_pem = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)

# Criptografia
message = b"Hello, RSA!"
ciphertext = public_key.encrypt(
    message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)

# Descriptografia
plaintext = private_key.decrypt(
    ciphertext,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)

print(f"Cipher Text: {ciphertext}")
print(f"Decrypted Text: {plaintext}")
```

Checklist

• Geração de p e q.

• Cálculo de n e φ(n).
• Escolha de e (chave pública).
• Cálculo de d (chave privada).
• Conversão da mensagem M em um número inteiro.
• Criptografia da mensagem M.

Checklist:

Apresentado ao final dos Procedimentos para a Realização da Atividade

Procedimento/Atividade nº 1 (Virtual)

Atividade proposta:

Nesta atividade, você aplicará seus conhecimentos sobre criptografia RSA, chaves pública e privada, e geração de chaves a partir de números primos. Vamos criar um cenário em que você precisa enviar uma mensagem segura para um amigo, utilizando criptografia RSA.

Procedimentos para a realização da atividade:

Passo 1: Geração de Chaves

Gere dois números primos grandes, p e q.

Para isso, você pode usar ferramentas online, como calculadoras de números primos.

Certifique-se de que p e q sejam números primos diferentes e mantenha esses valores em segredo.

Passo 2: Cálculo de n e φ(n)

Calcule n = p * q e φ(n) = (p-1)(q-1).

Mantenha esses valores em segredo.

Passo 3: Escolha da Chave Pública

Escolha um número e, em que 1 < e < φ(n), e que seja co-primo de φ(n).

Isso será sua chave pública (n, e).

Passo 4: Cálculo da Chave Privada

Calcule d, que é o inverso multiplicativo de e (mod φ(n)). Ou seja, d * e = 1 (mod φ(n)).

d será a sua chave privada.

Passo 5: Mensagem e Criptografia

Escolha uma mensagem M que você deseja enviar e converta-a em um número inteiro M.

Certifique-se de que M seja menor que n.

Criptografe a mensagem M utilizando a chave pública (n, e) e a fórmula: C = M^e (mod n).

O resultado, C, será a mensagem criptografada.

Passo 6: Descriptografia e Mensagem Decifrada

Envie C para o seu amigo.

Seu amigo deve possuir a chave privada (d) para descriptografar a mensagem. Para isso, ele usará a fórmula: M = C^d (mod n).

Sugestão de aplicação:

Para realizar essa atividade você pode usar a linguagem de programação Python e a biblioteca criptográfica "cryptography".

```python
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives import hashes

# Geração de chaves
private_key = rsa.generate_private_key(public_exponent=65537, key_size=2048

# Conversão das chaves em formato PEM
private_pem = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)

# Geração da chave pública
public_key = private_key.public_key()
public_pem = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)

# Criptografia
message = b"Hello, RSA!"
ciphertext = public_key.encrypt(
    message,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)

# Descriptografia
plaintext = private_key.decrypt(
    ciphertext,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
)

print(f"Cipher Text: {ciphertext}")
print(f"Decrypted Text: {plaintext}")
```

Checklist

• Geração de p e q.

• Cálculo de n e φ(n).

• Escolha de e (chave pública).

• Cálculo de d (chave privada).

• Conversão da mensagem M em um número inteiro.

• Criptografia da mensagem M.

• Descriptografia da mensagem C.

Checklist:

Apresentado ao final dos Procedimentos para a Realização da Atividade.

RESULTADOS

Resultados de Aprendizagem:

Após completar esta atividade, você deve ser capaz de compreender e aplicar os princípios da criptografia RSA, gerar chaves pública e privada a partir de números primos e realizar criptografia e descriptografia de mensagens

ROTEIRO DE AULA PRÁTICA

NOME DA DISCIPLINA: CRIPTOGRAFIA

Unidade: CRIPTOGRAFIA APLICADA A REDES DE COMPUTADORES

Seção: Assinatura digital

OBJETIVOS

Definição dos objetivos da aula prática:

• Compreender os conceitos e aplicações da assinatura digital.

• Realizar uma atividade prática complexa para criar uma assinatura digital.

• Aprender a validar documentos com assinaturas digitais.

• Conhecer a validade legal da assinatura digital no contexto do ICP-Brasil.

INFRAESTRUTURA

Instalações – Materiais de consumo – Equipamentos:

LABORATÓRIO DE INFORMÁTICA

Equipamentos:

• Desktop Lab Informatica - Positivo C6300

~ 1 un por grupo de alunos

SOLUÇÃO DIGITAL

• ADOBE ACROBAT READER (Software)

Adobe Reader é um software que permite que o usuário do computador visualize, navegue e imprima arquivos no formato PDF. Este tipo de arquivo é muito comum em documentações gerais. Por ser multiplataforma, está disponível para diversos sistemas operacionais.

EQUIPAMENTO DE PROTEÇÃO INDIVIDUAL (EPI)

Não se aplica

PROCEDIMENTOS PRÁTICOS

Procedimento/Atividade nº 1 (Físico)

Atividade proposta:

Nesta atividade prática, você aprenderá sobre a assinatura digital, sua importância, e como criar e validar uma assinatura digital. Também discutiremos a validade legal da assinatura digital no contexto do ICP-Brasil.

Procedimentos para a realização da atividade:

Passo 1: Criação de Assinatura Digital

Escolha uma mensagem ou documento que você deseja assinar digitalmente. Pode ser um arquivo de texto, PDF, ou qualquer formato que desejar.

Utilize uma ferramenta de assinatura digital, como o software Adobe Acrobat Reader ou uma ferramenta online, para criar uma assinatura digital do documento.

Siga as instruções da ferramenta para criar sua assinatura digital. Normalmente, isso envolve a criação de uma chave pública e privada.

Assine o documento digitalmente com sua chave privada.

Passo 2: Validação da Assinatura Digital

Envie o documento assinado digitalmente para um amigo ou colega.

Peça ao seu amigo ou colega para verificar a assinatura digital. Eles devem usar sua chave pública (que é publicamente disponível) para validar a assinatura.

Passo 3: Discussão sobre a Validade Legal

Pesquise e analise as regulamentações do ICP-Brasil em relação à assinatura digital e sua validade legal no Brasil.

Escreva um breve relatório sobre o que você descobriu, destacando os requisitos para que uma assinatura digital seja considerada válida e as aplicações práticas no contexto brasileiro.

Sugestão de aplicação:

Para criar e validar assinaturas digitais, você pode utilizar ferramentas como o Adobe Acrobat (para documentos PDF) ou serviços online de assinatura digital, como o DocuSign. Aqui está um exemplo de como criar uma assinatura digital usando o Adobe Acrobat:

Abra o documento no Adobe Acrobat.

Vá para "Ferramentas" e selecione "Proteger e Enviar".

Clique em "Assinar & Certificar" e escolha "Assinar com Certificado".

Siga as instruções para criar sua assinatura digital.

Checklist:

- Criação da assinatura digital.
- Assinatura do documento com a chave privada.
- Validação da assinatura digital usando a chave pública.
- Relatório sobre a validade legal da assinatura digital no ICP-Brasil.

Procedimento/Atividade nº 1 (Virtual)

Atividade proposta:

Nesta atividade prática, você aprenderá sobre a assinatura digital, sua importância, e como criar e validar uma assinatura digital. Também discutiremos a validade legal da assinatura digital no contexto do ICP-Brasil.

Procedimentos para a realização da atividade:

Passo 1: Criação de Assinatura Digital

Escolha uma mensagem ou documento que você deseja assinar digitalmente. Pode ser um arquivo de texto, PDF, ou qualquer formato que desejar.

Utilize uma ferramenta de assinatura digital, como o software Adobe Acrobat Reader ou uma ferramenta online, para criar uma assinatura digital do documento.

Siga as instruções da ferramenta para criar sua assinatura digital. Normalmente, isso envolve a criação de uma chave pública e privada.

Assine o documento digitalmente com sua chave privada.

Passo 2: Validação da Assinatura Digital

Envie o documento assinado digitalmente para um amigo ou colega.

Peça ao seu amigo ou colega para verificar a assinatura digital. Eles devem usar sua chave pública (que é publicamente disponível) para validar a assinatura.

Passo 3: Discussão sobre a Validade Legal

Pesquise e analise as regulamentações do ICP-Brasil em relação à assinatura digital e sua validade legal no Brasil.

Escreva um breve relatório sobre o que você descobriu, destacando os requisitos para que uma assinatura digital seja considerada válida e as aplicações práticas no contexto brasileiro.

Sugestão de aplicação:

Para criar e validar assinaturas digitais, você pode utilizar ferramentas como o Adobe Acrobat (para documentos PDF) ou serviços online de assinatura digital, como o DocuSign. Aqui está um exemplo de como criar uma assinatura digital usando o Adobe Acrobat:

Abra o documento no Adobe Acrobat.

Vá para "Ferramentas" e selecione "Proteger e Enviar".

Clique em "Assinar & Certificar" e escolha "Assinar com Certificado".

Siga as instruções para criar sua assinatura digital.

Checklist:

- Criação da assinatura digital.
- Assinatura do documento com a chave privada.
- Validação da assinatura digital usando a chave pública.
- Relatório sobre a validade legal da assinatura digital no ICP-Brasil.

RESULTADOS

Resultados de Aprendizagem:

Após completar esta atividade, você deve ser capaz de criar e validar assinaturas digitais, entender a validade legal da assinatura digital no contexto do ICP-Brasil e aplicar esses conhecimentos em situações práticas que exigem segurança e autenticidade de documentos.

NORMAS PARA ELABORAÇÃO E ENTREGA DO RELATÓRIO DE ATIVIDADE PRÁTICA

Olá, estudante. Tudo bem?
As atividades práticas visam desenvolver competências para a atuação profissional. Elas são importantes para que você vivencie situações que te prepararão para o mercado de trabalho.
Por isso, trazemos informações para que você possa realizar as atividades propostas com êxito.

1. Que atividade deverá ser feita?

- A(s) atividades a ser(em) realizada(s) estão descritas no Roteiro de Atividade Prática, disponível no AVA.
- Após a leitura do Roteiro, você deverá realizar a(s) atividade(s) prática(s) solicitadas e elaborar um documento **ÚNICO** contendo todas as resoluções de acordo com a proposta estabelecida.
- O trabalho deve ser autêntico e contemplar todas as resoluções das atividades propostas. Não serão aceitos trabalhos com reprodução de materiais extraídos da internet.

2. Como farei a entrega dessa atividade?

- Você deverá postar seu trabalho final no AVA, na pasta específica relacionada à atividade prática, obedecendo o prazo limite de postagem, conforme disposto no AVA.
- Todas as resoluções das atividades práticas devem ser entregues em um **ARQUIVO ÚNICO** de até 10 MB.
- O trabalho deve ser enviado em formato Word ou PDF, exceto nos casos em que há formato especificado no Roteiro.
- O sistema permite anexar apenas um arquivo. Caso haja mais de uma postagem, será considerada a última versão.

IMPORTANTE:

- A entrega da atividade, de acordo com a proposta solicitada, é um critério de aprovação na disciplina.
- Não há prorrogação para a postagem da atividade.

Aproveite essa oportunidade para aprofundar ainda mais seus conhecimentos.

Bons estudos!