UNIVERSIDADE FEDERAL DO AGRESTE DE PERNAMBUCO - UFAPE
BACHARELADO EM CIÊNCIAS DA COMPUTAÇÃO

IZABEL YALE NEVES NASCIMENTO

JONAS FERREIRA LEAL JUNIOR

A IMPORTÂNCIA DA ASSINATURA DIGITAL NA DIGITALIZAÇÃO DOS PROCESSOS: RELATÓRIO FINAL DA DISCIPLINA EM SEGURANÇA DE REDE EM COMPUTADORES

GARANHUNS

2024

SUMÁRIO

1. INTRODUÇÃO

Com a crescente digitalização da comunicação e dos processos, se faz necessário assegurar a confiabilidade e a integridade das informações nesse meio digital, assim como já acontece no ambiente físico. Neste cenário, surge a Assinatura Digital como uma ferramenta essencial para prover essa garantia, pois permite que seja checado, de forma simples e eficiente, se houve alterações no objeto assinado após o momento da assinatura. Seu avanço e segurança está intrinsecamente ligado ao uso de criptografia, pois essa tecnologia desempenha um papel crucial no processo de assinatura digital. Como ressalta Stallings (2015, p. 310), “o desenvolvimento mais importante a partir do trabalho sobre criptografia de chave pública é a assinatura digital. Esta oferece um conjunto de capacidades de segurança que seria difícil de implementar de qualquer outra maneira”.

A integridade dos processos digitais é garantida pela assinatura digital, já que esta utiliza técnicas de criptografia para proteger os documentos contra adulteração. Por meio de chaves pública e privada, a assinatura digital assegura que seja possível identificar qualquer modificação em documentos ao longo do tempo. Isso é especialmente relevante quando falamos de ambientes nos quais a confiança na autenticidade dos documentos é de suma importância, como em contratos comerciais, documentos legais e registros médicos.

A assinatura digital também proporciona segurança, pois a utilização da criptografia no processo faz com que cada uma das chaves utilizadas no processo seja única e muito difícil de serem replicadas, diferente de assinaturas manuscritas ou carimbos que podem ser facilmente falsificados. Isso garante que apenas as partes autorizadas possam assinar digitalmente um documento, reduzindo assim o risco de adulterações e fraudes. Além disso, a assinatura digital contribui para a eficiência dos processos ao eliminar impressões, envio físico, armazenamento de documentos em papéis e diminuindo algumas burocracias, como a assinatura em massa de documentos.

2. MOTIVOS PARA USAR, VANTAGENS E DESVANTAGENS

Vantagens:

Como já foi mencionado antes, a assinatura digital apresenta vantagens como a de garantir a autenticidade, integridade, segurança, uma vez que imputa um autor da assinatura, permite rastrear alterações e realizar checagens de maneira prática. Também é um método mais eficiente do ponto de vista operacional, pois possibilita automatizar o processo de assinatura, reduz erros, proporciona economia de recursos e tempo. Pode ser facilmente implantado em diversos dispositivos, trazendo maior mobilidade, permitindo que um documento seja assinado remotamente e mantendo sua aceitação legal.

Desvantagens:

A assinatura digital é reconhecida pela sua eficiência e segurança, porém, é importante entender que existem pontos negativos relacionados ao seu uso, como por exemplo: a assinatura digital depende da tecnologia, sendo que nem todos têm acesso ou conhecimento para o seu uso. Além disso, pode existir custos para aquisição e manutenção da assinatura bem como do dispositivo para o uso. Outro ponto é o conhecimento da população sobre o assunto e a confiança para o uso, que pode levar um tempo elevado para a aceitação e uso. Assim também, a sua segurança está atrelada a eficiência da criptografia envolvida no processo, dessa forma, se for encontrado uma forma prática de quebrar essa criptografia, a assinatura digital que a utiliza estará vulnerável.

Motivos para usar:

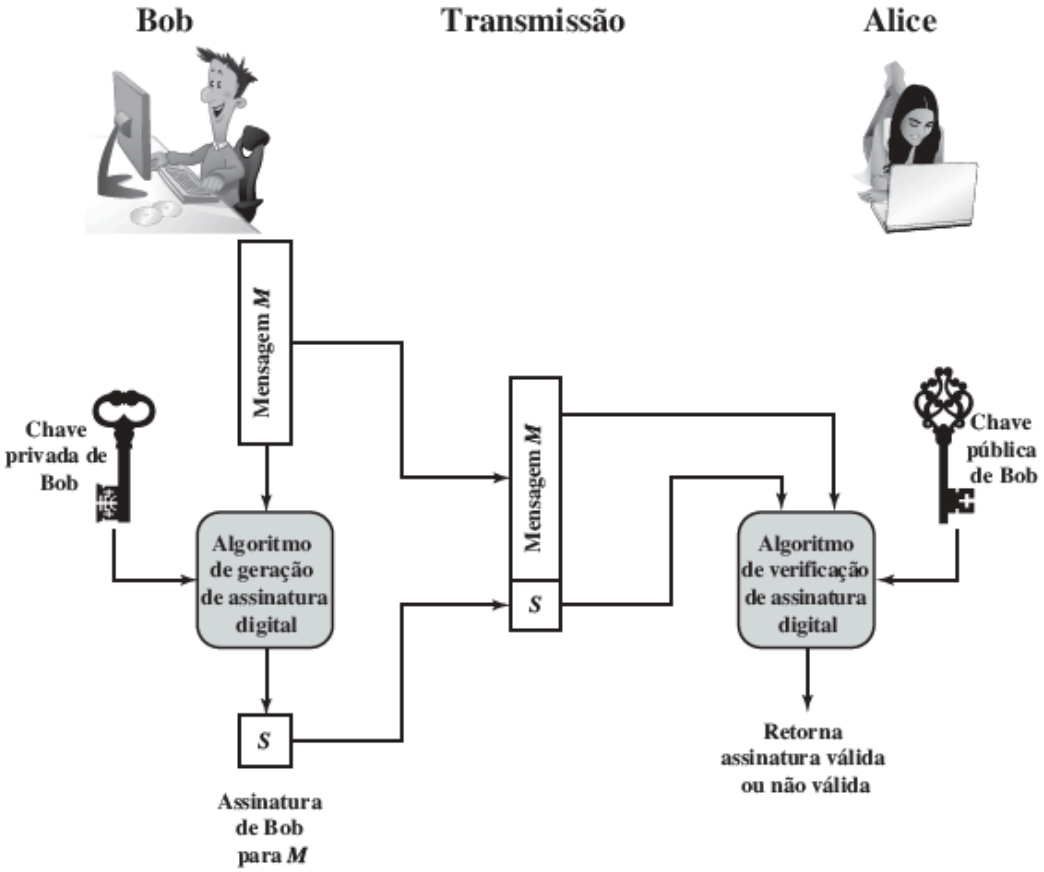
Apesar de apresentar algumas desvantagens, as implementações atuais da assinatura digital apresentam uma boa confiabilidade e tem sido encorajado o uso desta por meio de política pública - que disponibiliza a possibilidade de assinar digitalmente documentos de forma gratuita -, e pela redução dos preços da aquisição de um certificado digital, que permite a assinatura.

3. A SOLUÇÃO

3.1 Esquema de assinatura digital genérica

O esquema de assinatura envolve o uso da chave privada para encriptação e a chave pública para decriptação. Abaixo, observa-se a representação genérica do uso de um algoritmo de geração de assinatura digital.

Figura 1: Exemplo de geração de assinatura digital.



Fonte: Retirado do livro “Criptografia e segurança de rede”, William Stallings, 2015.

Na Figura 1, usando um algoritmo de assinatura digital, Bob pode assinar uma mensagem enviando-a como entrada e uma chave privada, essa por sua vez irá gerar uma chave pública para uma futura descriptografia. Qualquer outro usuário, digamos, Alice, pode verificar a assinatura usando um algoritmo de verificação, cujas entradas são a mensagem, a assinatura e a chave pública de Bob.

Para entendimento das soluções existentes para algoritmos de assinatura digital é importante orientar-se pela seguinte ordem: Elgamal, Schnorr e algoritmos do NIST.

4. MAIOR DETALHAMENTO DA SOLUÇÃO

4.1 Esquema de assinatura digital Elgamal

O esquema de assinatura digital Elgamal faz uso de chave privada para encriptação de chave pública para decriptação, assim como apresentado no esquema genérico anteriormente. Segue os passos do esquema:

Configuração para a assinatura:

- Escolha de um primo *q* para ser o corpo *GF(q)* (quanto maior melhor);
- Calcular uma raiz primitiva desse primo (para um valor *x* ser raiz primitiva todos os resultados de *x^n* sendo *n 1* até *p-1* devem ser resultados diferentes).

Par de chaves:

- A pessoa escolhe sua chave privada *(X)*;
- Define-se uma raiz primitiva *a*;
- A partir da sua chave privada e da configuração para a assinatura, é formada a chave pública *{q, a, Y}*.

Envio da mensagem (criptografia):

- Define-se uma assinatura para transmissão *m*;
- Escolhe um *k* primo relativo;
- Calcula-se *S1 = (a^k) mod q*;
- Calcula-se *S2 = k^(-1) (m - X*S1) mod (q - 1)*;

Recebimento da mensagem (descriptografia):

- Identifica-se a mensagem *V1 = (a^m) mod q;*
- Valida a assinatura *V2 = Y^(S1) S1^(S2) mod q.*

Exemplo prático: começando com o corpo primo GF(19); ou seja, q = 19. Ele tem raízes primitivas {2, 3, 10, 13, 14, 15}. Escolhemos a = 10.

Alice gera um par de chaves da seguinte forma:

1. Alice escolhe XA = 16.
2. Então YA = a^(XA) mod q = a^16 mod 19 = 4.
3. A chave privada de Alice é 16; a chave pública de Alice é {q, a, YA} = {19, 10, 4}.

Suponha que Alice queira assinar uma mensagem com valor de hash m = 14.

1. Alice escolhe K = 5, que é relativamente primo de q – 1 = 18.
2. S1 = a^K mod q = 10^5 mod 19 = 3.
3. K^(–1) mod (q – 1) = 5^(–1) mod 18 = 11.
4. S2 = K^(–1) (m – XAS1) mod (q – 1) = 11 (14 – (16)(3)) mod 18 = –374 mod 18 = 4.

Bob pode verificar a assinatura da seguinte forma:

1. V1 = a^m mod q = 10^14 mod 19 = 16.
2. V2 = (YA)^(S1) * (S1)^(S2) mod q = (4^3)(3^4) mod 19 = 5184 mod 19 = 16.

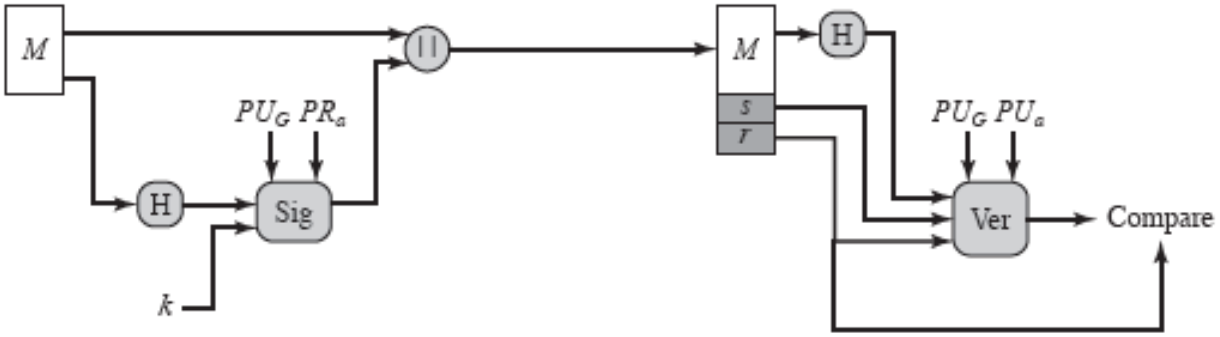
Assim, a assinatura é válida.

4.2 Algoritmo de assinatura digital do NIST

O National Institute of Standards and Technology (NIST) publicou o algoritmo de assinatura digital (Digital Signature Algorithm — DSA) que faz uso do Secure Hash Algorithm (SHA).

O DSA é baseado na dificuldade de se calcular logaritmos discretos e é baseado nos esquemas Elgamal e Schnorr apresentados anteriormente. Observa-se uma imagem do funcionamento do algoritmo.

Figura 2: Técnica de criptografia do DSA.



Fonte: Retirado do livro “Criptografia e segurança de rede”, William Stallings, 2015.

Analisando a parte esquerda da Figura 2, para a criptografia da mensagem clara *M*, é fornecido o código de hash *(H)* como entrada de uma função de assinatura *(Sig)*, junto com um número aleatório *k*, gerado para essa assinatura em particular. A função de assinatura também depende da chave privada do emissor *(PRa)* e um conjunto de parâmetros conhecidos de um grupo de membros em comunicação. Podemos considerar esse conjunto como constituindo de uma chave pública global *(PUG)*. O resultado é uma assinatura que consiste em dois componentes, rotulados com “s” e “r”.

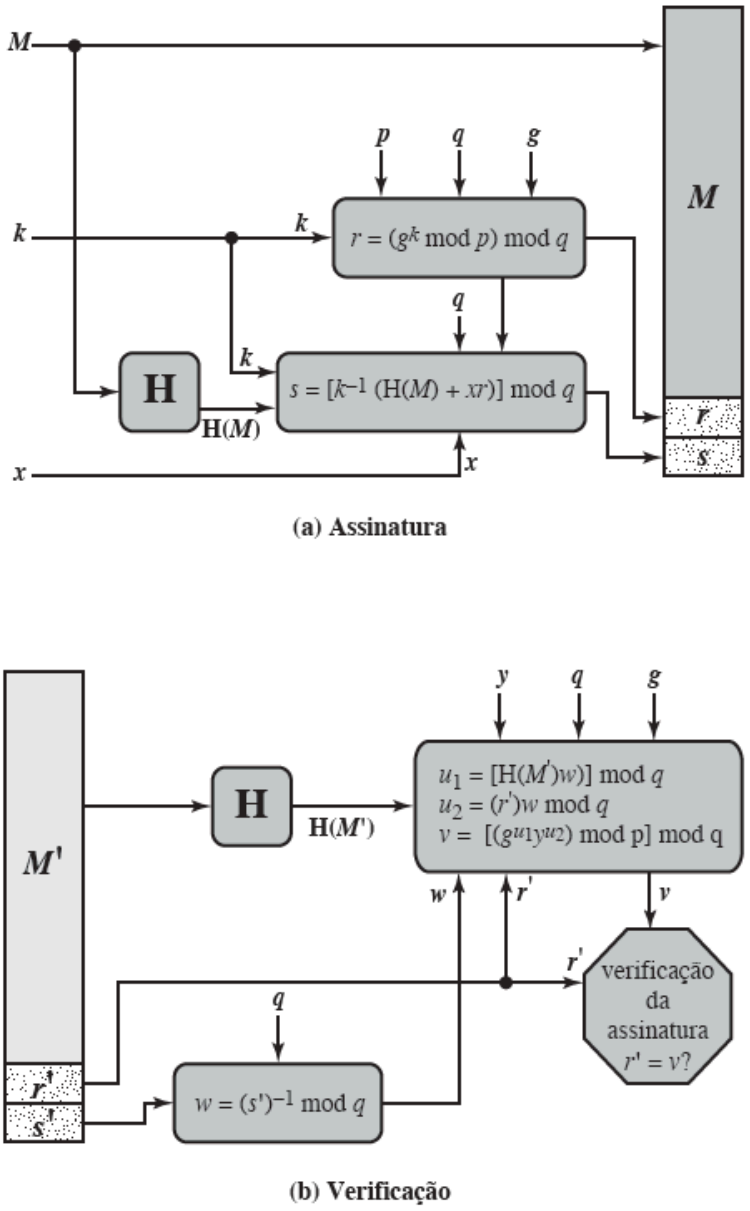
Já na parte direita da Figura 2, após a mensagem *M* chegar, é passado pelo algoritmo *H* com pública global *(PUG)* e a chave pública do emissor *(PUa)*, então ocorre a verificação *(Ver)* a mensagem clara é obtida e passa pelo processo de validação.

Esse algoritmo mantém o padrão de funcionamento, seguindo os passos:

1 - Geração de chaves;
2 - Geração dos parâmetros;
3 - Assinatura;
4 - Verificação;
5 - Validação.

Os processos de Assinatura (Sig) e Verificação (Ver) podem ser observados com mais detalhes na Figura 3 abaixo.

Figura 3: Esquema detalhado.



Fonte: Retirado do livro “Criptografia e segurança de rede”, William Stallings, 2015.

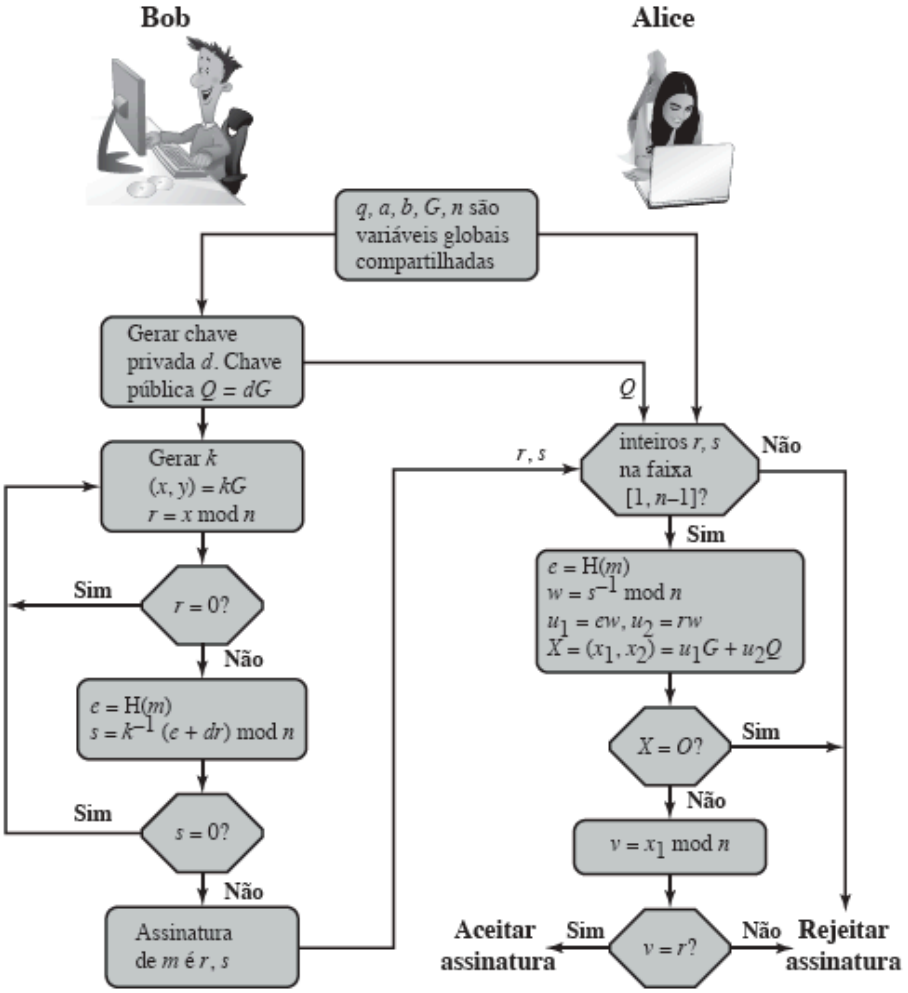
4.2 Algoritmo de assinatura digital de Curva Elíptica

Elliptic Curve Digital Signature Algorithm (ECDSA) está obtendo cada vez mais aceitação por causa da vantagem de eficiência da criptografia de curva elíptica, que gera segurança comparável à de outros esquemas com um tamanho de chave menor em quantidade de bits. Etapas:

1 - Parâmetros de domínio global: parâmetros que definem uma curva elíptica e um ponto de origem nela;
2 - Geração de chave: gerar um par de chaves pública e privada. Para a chave privada, é selecionado um número aleatório ou pseudo aleatório. Usando esse número aleatório e o ponto de origem, o assinante calcula outro ponto na curva elíptica. Essa é a chave pública.

3 - Geração e autenticação de assinatura digital: um valor de hash é gerado para a mensagem ser assinada. Usando a chave privada, os parâmetros de domínio e o valor de hash, a assinatura é gerada. A assinatura consiste em dois inteiros, “r” e “s”.
4 - Verificação: o verificador usa como entrada a chave pública do assinante, os parâmetros do domínio e o inteiro s. A saída é um valor “v” que é comparado com “r”. A assinatura é válida se “v = r”.

Figura 4: Esquema finalizado.



Fonte: Retirado do livro “Criptografia e segurança de rede”, William Stallings, 2015.

5. Implementações

- Link da implementação do Elgamal: https://github.com/izabelnascimento/seguranca-redes-ufape/blob/main/2-VA/cifra_elgamar.py
- Link da implementação do ECDSA baseada em Moreira (2006, p. 8): https://github.com/izabelnascimento/seguranca-redes-ufape/tree/main/2-VA/ecdsa

6. Conclusões

Após entender a importância da assinatura digital, visitar seus prós e contras e analisar as soluções contendo três esquemas de assinatura digital: Elgamal, Algoritmo de Assinatura Digital do NIST (DSA) e Elliptic Curve Digital Signature Algorithm (ECDSA), podemos concluir que cada um deles apresenta suas próprias características e vantagens.

Elgamal utiliza criptografia de chave pública baseada em logaritmos discretos. Ele oferece segurança contra ataques de força bruta, desde que a escolha dos parâmetros seja feita adequadamente. Além disso, é flexível e pode ser adaptado para diferentes tamanhos de chaves.

Algoritmo de Assinatura Digital do NIST (DSA) é baseado nos esquemas Elgamal e Schnorr. Ele utiliza o Secure Hash Algorithm (SHA) para garantir a integridade da mensagem e é amplamente utilizado em aplicações que requerem assinaturas digitais seguras.

Elliptic Curve Digital Signature Algorithm (ECDSA) aproveita a eficiência da criptografia de curva elíptica, proporcionando segurança comparável com chaves menores em relação a outros esquemas. Ele é amplamente utilizado em aplicações que demandam eficiência e segurança, como sistemas de pagamento eletrônico e comunicações seguras.

Em resumo, cada esquema de assinatura digital tem suas próprias características e aplicações específicas. A escolha entre eles dependerá das necessidades e requisitos de segurança do sistema em questão.

Referências

MOREIRA, Márcio Aurélio Ribeiro. (2006). **"ECDSA (Elliptic Curve Digital Signature Algorithm)"** Uberlândia, MG. Acessado e recuperado de <https://www.inf.ufsc.br/~bosco.sobral/ensino/ine563-0/material-cripto-seg/crpt_trabalho_ecdsa.pdf>. Acesso em 15 fev 2024.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. – São Paulo: Pearson Education do Brasil, 2015.