

Professor: Calvetti

Apresentação Atividade 4

CRIPTOGRAFIA

São Paulo
2024

Participantes do grupo:

Anabelly Rocha

Carolina Cruz

Maria Eduarda

Códigos Navajos

Os códigos navajos foram um sistema de comunicação utilizado durante a Segunda Guerra Mundial, criado por soldados navajos para transmitir mensagens de forma segura e rápida. Essa linguagem codificada aproveitava a rica cultura navaja, incluindo termos específicos da fauna, flora e do cotidiano, tornando-a incompreensível para quem não falasse a língua navaja.

Os navajos foram recrutados pelo Exército dos EUA, e seu sistema de códigos foi essencial para a comunicação em batalhas, especialmente no Pacífico. A eficiência desse método se deve à sua complexidade e à falta de conhecimento da língua navaja por parte dos inimigos, o que dificultava a interceptação e decodificação das mensagens.

Essa inovação na criptografia não apenas contribuiu para vitórias militares, mas também destacou a importância e o valor da cultura navaja. Os códigos navajos permaneceram em uso mesmo após a guerra, sendo um símbolo de resistência e identidade cultural.

Letter	Navajo word	English word
C	MOASI	Cat
D	LHA-CHA-EH	DOG
E	DZEH	Elk
I	TKIN	Ice
O	NE-AHS-JAH	Owl
R	GAH	Rabbit
V	A-KEH-DI-GLINI	Victor

Código de Scytale (Cítala)

- **Definição:** A scytale é uma ferramenta de criptografia da Grécia antiga, usada para enviar mensagens codificadas.
 - **Funcionamento:** Consiste em um bastão (scytale) ao qual uma tira de pergaminho é enrolada. A mensagem é escrita ao longo do bastão; quando desenrolada, fica ilegível sem um bastão do mesmo diâmetro.
 - **Segurança:** A cifra é simples, mas eficaz, pois a mensagem só pode ser lida com a scytale correta, garantindo a confidencialidade.
 - **História:** Usada por militares para transmitir ordens de forma segura, exemplificando a aplicação da criptografia em contextos de guerra.



CHAVES SIMÉTRICAS

AES (Advanced Encryption)

O AES é uma variação da família Rijndael de algoritmos de criptografia simétrica de bloco, cujo nome é uma combinação dos sobrenomes dos criptógrafos belgas Joan Daemen e Vincent Rijmen, semelhante às combinações de nomes de celebridades como "Brangelina" ou "Kimye".

A criptografia AES é amplamente utilizada em várias aplicações, como segurança sem fio, proteção de processadores, criptografia de arquivos e protocolos SSL/TLS.

O Instituto Nacional de Padrões e Tecnologia (NIST) estabeleceu o AES como padrão de criptografia há quase 20 anos, em substituição ao antigo DES.

O sucesso do AES foi tão grande que muitas entidades e agências o aprovaram e o utilizam para criptografar dados sensíveis.

Data Encryption Standard (DES)

O Data Encryption Standard (DES) é um algoritmo de criptografia simétrica criado nos anos 1970 para garantir a segurança de dados. Foi o primeiro método de criptografia a se tornar padrão tanto nos Estados Unidos quanto internacionalmente. Essencialmente, o DES realiza duas operações principais em sua entrada: o deslocamento e a substituição de bits.

A chave determina exatamente como esse processo é executado. Ao repetir essas operações de forma não linear, obtém-se um resultado que não pode ser revertido para a entrada original sem a chave.

Principais características do DES:

- Uma das principais características do DES é a sua simplicidade. Apesar de ser um algoritmo antigo, ele ainda é amplamente utilizado devido à sua eficácia e facilidade de implementação. Além disso, o DES é um algoritmo rápido, o possibilitando para criptografar grandes volumes de dados em tempo real.
- O DES também é conhecido por sua resistência a ataques de força bruta.

Impasses:

- O tamanho da chave é considerado pequeno.
- Possui vulnerabilidade a ataques diferencias: esses ataques exploram padrões estatísticos nos dados criptografados para deduzir informações sobre a chave de criptografia.

CHAVES ASSIMÉTRICAS



RSA

No ano de 1977 Riverst, Shamir e Adleman desenvolveram um dos algoritmos assimetrico mais utilizados atualmente, nomeado de RSA, sendo o nome do algoritmo uma homenagem para o seus criadores.

A criptografia RSA utiliza números muito maiores. Por exemplo, em um sistema RSA de 2048 bits, as chaves possuem 617 dígitos. As funções de porta de armadilha são fundamentais para o funcionamento dos esquemas de criptografia de chave pública e privada.

A RSA funciona da seguinte forma: **Geração de Chaves**

É selecionado dois números primos grandes, p e q .

- Escolha de Primos: Selecionam-se dois números primos grandes, p e q
- Multiplica-se p e q para obter n (ou seja, $n=p \times q = p \times q$).
- Cálculo de $\phi(n)$: Calcula-se $\phi(n)=(p-1)(q-1)$.
- Escolhe-se um número e que seja coprimo a $\phi(n)$ e que satisfaça $1 < e < \phi(n)$ (geralmente $e=65537$).
- Cálculo de d : Encontra-se d como o inverso multiplicativo de e módulo $\phi(n)$.

RSA

Chaves

- Chave Pública: Composta por (n, e) .
- Chave Privada: Composta por (n, d) .

Criptografia

- Para criptografar uma mensagem m (convertida em um número inteiro), calcula-se: $c \equiv m^e \pmod{n}$

Descriptografia

- Para recuperar a mensagem m , usa-se: $m \equiv c^d \pmod{n}$

Segurança

A segurança do RSA está na dificuldade de fatorar o produto de dois números primos grandes. Mesmo conhecendo n e e , fatorar n para descobrir p e q é extremamente difícil.

Criptografia Diffie-Hellman

A criptografia Diffie-Hellman é um método de troca de chaves que permite que duas partes estabeleçam uma chave secreta compartilhada por meio de um canal inseguro, utilizada para criptografar comunicações futuras.

Princípios Básicos

Baseia-se na dificuldade do problema do logaritmo discreto, envolvendo números primos e operações modulares.

Etapas do Processo

Escolha de Parâmetros: As partes concordam em um número primo grande p e uma base g (pública).

Segurança:

A segurança provém da dificuldade de derivar as chaves privadas a partir das chaves públicas.

Exemplo:

Geração de Chaves Privadas: Alice escolhe a e Bob escolhe b como chaves privadas.

Cálculo de Chaves Públicas:

Alice calcula $A = g^a \text{ mod } p$

Bob calcula $B = ab \text{ mod } p$

Trocaram A e B

Cálculo da Chave Secreta Compartilhada:

Alice calcula $S = B^a \text{ mod } p$

Bob calcula $S = A^b \text{ mod } p$

Os dois conseguem a mesma chave secreta S .

REFERÊNCIAS BIBLIOGRÁFICAS

<https://cryptoid.com.br/criptografia/aes-padrao-de-criptografia-avancado-o-que-e-e-como-funciona/>

<https://expressvps.com.br/glossario/o-que-e-data-encryption-standard-des/>

https://www.gta.ufrj.br/grad/06_1/ssl/cripto.htm#:~:text=Os%20principais%20algoritmos%20de%20criptografia%20assim%C3%A9trica%20s%C3%A3o%20RSA%2C%20Diffie%2DHelman,%C3%BAltimo%20n%C3%A3o%20suportado%20pelo%20TLS.

<https://www.ibm.com/docs/pt-br/aix/7.3?topic=authentication-diffie-hellman-encryption>

<https://zheit.com.br/post/o-codigo-nunca-decifrado-na-ii-guerra>

<https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/>