UNIVERSIDADE SÃO JUDAS TADEU

GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

NATASHA MELO E YASMIN VICTÓRIA

# **Lucifer: A Cifra que Influenciou a Criptografia Moderna**

**SÃO PAULO**

**2024**

NATASHA MELO E YASMIN VICTÓRIA

RA:82429222 E 824210011

# **Lucifer: A Cifra que Influenciou a Criptografia Moderna**

**SÃO PAULO**

**2024**

# **Lucifer: A Cifra que Influenciou a Criptografia Moderna**

**Prática 4**

**Introdução**

Lucifer é uma cifra histórica que surgiu nos anos 1970, desenvolvida pela IBM e que teve um papel fundamental na evolução da criptografia digital. Embora não seja tão conhecida quanto o DES, sua influência é inegável.

O que é Lucifer?

Criada por uma equipe liderada por Horst Feistel, Lucifer foi uma das primeiras cifras modernas projetadas para proteger dados digitais. O algoritmo foi desenvolvido para sistemas de segurança e se destacou pela sua estrutura de cifra de blocos.

Características Principais Cifra de Blocos:

Lucifer opera dividindo os dados em blocos de um tamanho fixo, inicialmente de 48 bits, mas depois ajustado para 64 bits. Cada bloco é processado individualmente, garantindo segurança.

Criptografia Simétrica:

A cifra usa a mesma chave tanto para cifrar quanto para decifrar. Isso significa que tanto quem envia quanto quem recebe a mensagem precisam compartilhar a mesma chave secreta. Rede Feistel: Lucifer utiliza uma técnica chamada rede Feistel, que divide os blocos de dados e os processa em várias rodadas, alternando entre substituições e permutações. Isso ajuda a criar um resultado cifrado que é muito diferente do texto original.

Impacto no DES:

A cifra Lucifer chamou a atenção da Agência Nacional de Segurança dos EUA (NSA), que colaborou com a IBM para criar uma versão mais robusta do algoritmo, resultando no DES (Data Encryption Standard), lançado em 1977. O DES se tornou amplamente utilizado em várias áreas, especialmente em transações financeiras.

Conclusão:

Embora Lucifer não tenha sido adotada amplamente em sua forma original, sua importância na história da criptografia moderna é inegável. Ela ajudou a abrir caminho para algoritmos de segurança mais complexos e eficazes, marcando a transição da criptografia clássica para a digital. Em resumo, Lucifer foi um passo crucial na jornada da segurança da informação.

**Fonte de Referência**

Para mais detalhes sobre a cifra Lucifer, consulte a <https://cryptoid.com.br/> e <https://www.convectiva.com/>.

**Cifra de Jefferson**

Desenvolvido em 1795, por Thomas Jefferson (1743-1826), é um algoritmo bem simples: composto por 36 discos e um eixo, cada disco tem 26 letras do alfabeto aleatório na sua borda. O emissor coloca os discos no eixo e junta as letras em pares, numa linha de mensagem com 26 filas de letras. Então isso facilita, porque cada linha subliminar é codificada pelas outras 25 fileiras de letras.

O receptor codifica os códigos, apenas alinhando as letras aleatórias enviadas, e procura uma linha que faça sentido. Lembrando que quem envia os discos e quem o recebe, devem ficar empilhados na mesma ordem para facilitar a interpretação dos códigos. Sendo essa a chave da criptografia.

A complexidade da cifra é tão demasiada, que muitos códigos do sistema não foram descoberto até os dias atuais.

Uma das cifras que constituem a cifra de Jefferson, foi a cifra do criptólogo Joseph Mauborgne, uma versão mais segura da tal cifra, em 1915.

**Fonte de Referência**

Para mais detalhes consulte a <https://www.blogs.unicamp.br/>

# **Criptografia com Chaves Assimétricas:**

* Criptografia de Curva Elíptica (ECC)

A Criptografia de Curva Elíptica (ECC) representa uma abordagem contemporânea de criptografia assimétrica que aproveita as propriedades das curvas elípticas para proteger comunicações. Em comparação ao RSA, a ECC alcança um nível semelhante de segurança utilizando chaves menores, resultando em maior eficiência e rapidez. Essa eficiência a torna ideal para dispositivos com recursos limitados, como smartphones e aplicações em IoT.

* Criptografia RSA (Rivest-Shamir-Adleman)

O algoritmo RSA (Rivest-Shamir-Adleman) é uma das principais técnicas de criptografia assimétrica, baseado na dificuldade de fatorar números grandes. Ele utiliza um par de chaves: uma chave pública, que pode ser compartilhada livremente, e uma chave privada, que é mantida em segredo. Essa estrutura permite que dados sejam criptografados e assinaturas digitais sejam verificadas de forma segura. A segurança do RSA é crucial em protocolos como SSL/TLS, que protegem comunicações na internet e autenticação de usuários. Apesar de sua eficácia, a crescente ameaça da computação quântica impulsiona pesquisas em métodos para fortalecer e substituir o RSA, garantindo a segurança futura das informações.

**Fonte de Referência**

Para mais detalhes consulte a <https://cryptoid.com.br/>.

# **Criptografia com Chaves Simétricas:**

* Criptografia AES (Advanced Encryption Standard - Padrão de Criptografia Avançada)

\* AES (Advanced Encryption Standard - Padrão de Criptografia Avançada):

É um algoritmo desenvolvido para proteger dados eletrônicos. Suas chaves criptográficas é de 128, 192 e 256 bits. É uma criptografia altamente segurança, exceto a ataques de força bruta.

* Criptografia DES (Data Encryption Standard):

\* DES (Data Encryption Standard):

Uma das criptografias mais usadas, é o DES um algoritmo de baixa proteção, com apenas 56 bits capaz de cifrar e decifrar dados. Foi criado com objetivo de proteger informações sigilosas, sendo pessoais, financeiras e comerciais.

**Fonte de Referência**

Para mais detalhes consulte a <https://www.codia.com.br/glossario/o-que-e-data-encryption-standard-des/>, <https://v3technology.com.br/glossario/o-que-e-data-encryption-standard-des/>