ATIVIDADE 04

Docente: Robson Calvetti

UC: Sistemas Computacionais e Segurança – SCS

Grupo

Marinna Pereira Carneiro da Silva - RA: 824142121

Mariana Hildebrand Dantas - RA: 824118462

Christian Batista de Lima - RA: 824126605

Beatriz Silva de Jesus – RA: 824219590

Análise e Desenvolvimento de Sistemas – ADS

Trabalho realizado sobre a atividade da aula ocorrida em 17/09/24.

• Pesquisar, Entregar e Apresentar:

❑ Escolher 2 (dois) exemplos históricos do uso de criptografia não citados neste material;

❑ Citar 2 algoritmos de Criptografia com Chaves Simétricas utilizados atualmente;

❑ Citar 2 algoritmos de Criptografia com Chaves Assimétricas utilizados atualmente;

1º exemplo

O Código Navajo: Uma comunicação indecifrável criada por indígenas na 2º Guerra Mundial.

Os Marines (Fuzileiros Navais) dos EUA usaram falantes nativos da língua navajo para criar um código que fosse indecifrável para os inimigos durante a Segunda Guerra Mundial. Os Navajos desenvolveram um sistema de comunicação que utilizava palavras em sua língua para representar termos militares e conceitos estratégicos. Esse código foi crucial em batalhas como a de Iwo Jima, contribuindo significativamente para o sucesso militar dos aliados.

O grupo ficou conhecido como **Navajo Code Talkers**, no inglês. A princípio, era um pequeno grupo de 29 recrutas do povo indígena navajo, porém, com o sucesso do código durante a guerra, esse número chegou a mais de 400 homens ao seu término. Eles atribuíram nomes de clãs a unidades militares, usaram nomes de animais para aviões e até mesmo criaram um alfabeto onde cada letra correspondia a uma palavra Navajo.

Com mais de 400 palavras codificadas e um alfabeto Navajo-Inglês para soletrar coisas que não estavam no vocabulário, esses recrutas estavam prontos. Ao que conta a história, o impacto dos **Navajo Code Talkers** foi imenso. Em batalhas como Iwo Jima, eles enviaram mais de 800 mensagens em apenas dois dias, todas sem errar uma única palavra sequer. Um major chegou a dizer que, sem eles, os fuzileiros navais nunca teriam tomado Iwo Jima.

A batalha de Iwo Jima que os **Navajo Code Talkers** participaram, foi uma batalha datada em 1945, em que os Estados unidos (Fuzileiros Navais, mais especificamente falando) desembarcaram e conquistaram essa ilha, até então, pertencente ao Japão, durante a Segunda Guerra Mundial. A batalha foi denominada como **Operação Detachment**, e tinha como objetivo principal a conquista da ilha por conta de seus 3 aeroportos presentes, fazendo com que se tornasse então, uma base americana e dali, ficasse mais próximo para se atacar as principais localidades japonesas.

Fontes usadas:

Código Navajo:
https://www.megacurioso.com.br/artes-cultura/codigo-navajo-a-comunicacao-indecifravel-criada-por-indigenas-na-2-guerra-mundial

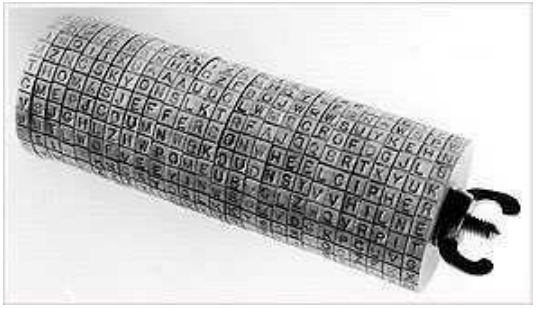
Batalha em Iwo Jima: https://pt.wikipedia.org/wiki/Batalha_de_Iwo_Jima

2º exemplo

As cifras criadas por Thomas Jefferson, 3º presidente dos Estados Unidos.

Um dos melhores e mais simples modelos de cifra foi criado por um advogado, revolucionário, diplomata, enólogo, arqueólogo e mais tarde presidente dos Estados Unidos. Além de inventar um país, Thomas Jefferson (1743-1826) ainda teve tempo para se dedicar à criptografia.

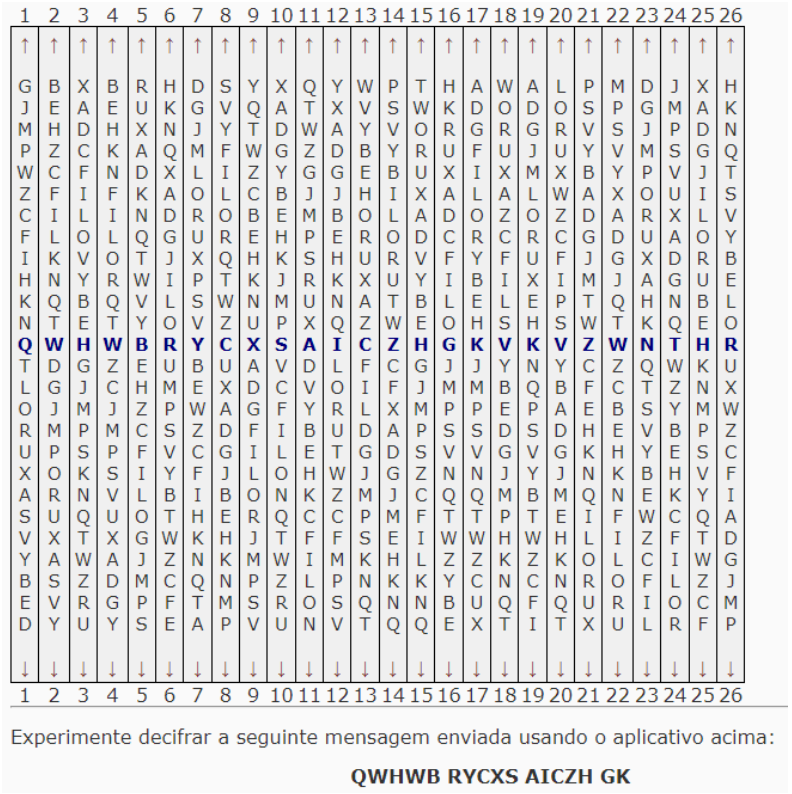
Na época em que era secretário de estado de George Washington, Thomas Jefferson, futuro presidente dos Estados Unidos, criou um método simples, engenhoso e seguro de cifrar e decifrar mensagens: o cilindro cifrante. A cifra de Jefferson é simples: um conjunto de 36 discos e um eixo. Cada um desses discos tem as 26 letras do alfabeto estampadas aleatoriamente na sua borda. O emissor empilha os discos no eixo e emparelha as letras de modo que uma linha da mensagem possa ser lida em uma das 26 filas de letras. Isso permite que cada linha da mensagem seja instantaneamente codificada pelas outras 25 fileiras de letras — basta escolher uma dessas fileiras de letras aleatórias, copiá-la e mandar a mensagem.



Quem recebe a mensagem faz a decodificação com o mesmo conjunto de discos. Basta alinhar as letras aleatórias enviadas e procurar por uma linha que faça sentido. Evidentemente, os discos do emissor e do receptor devem estar empilhados na mesma ordem.

É aí que está a chave da criptografia de Jefferson. Mas mesmo se os discos da cifra caírem em mãos erradas a mensagem vai ficar segura. É inútil ter os discos sem saber exatamente qual a ordem em que eles foram empilhados pelo emissor. Deveras inútil: os 36 discos podem ser empilhados de 371.993.326.789.901.217.467.999.448.150.835.200.000.000 maneiras distintas.

Segue um exemplo abaixo, de como seria feita a codificação dessa cifra:



Fontes usadas:

https://www.blogs.unicamp.br/hypercubic/2014/02/a-cifra-de-jefferson/

http://numaboa.com.br/criptografia/substituicoes/polialfabeticas/804-jefferson

2 Algoritmos de Criptografia com chaves Simétricas utilizados ultimamente:

AES (Advanced Encryption Standard)

Desenvolvido em 2001 como resultado de uma competição organizada pelo NIST para substituir o DES, é amplamente utilizado para proteger dados em várias aplicações, considerado um algoritmo de criptografia simétrica popular. Ele oferece combinações de chaves com 128, 192 ou 256 bits para criptografar blocos de dados de 128, 192 ou 256 bits.

IDEA (International Data Encryption Algorithm)

Criado por James Massey e Xuejia Lai em 1991, o IDEA foi desenvolvido para superar as limitações do DES (Data Encryption Standard), especialmente em relação ao tamanho da chave e à segurança. A necessidade de um algoritmo que pudesse oferecer segurança robusta e eficiência motivou a sua criação. Operando em blocos de 64 bits, ele utiliza uma chave de 128 bits, o que é significativamente mais seguro que o DES. O IDEA é utilizado principalmente em aplicações de criptografia de dados, como em PGP (Pretty Good Privacy), garantindo a segurança e confidencialidade de mensagens e informações sensíveis.

2 Algoritmos de Criptografia com chaves Assimétricas utilizados ultimamente:

RSA (Rivest-Shamir-Adleman)

Desenvolvido em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman, o RSA é um algoritmo de criptografia de chave pública que se baseia na dificuldade de fatorar números primos muito grandes. É amplamente utilizado em protocolos de comércio eletrônico e acredita-se ser seguro, dadas as chaves suficientemente longas, comumente tendo até 2048 bits. É muito utilizado também para criptografia de dados, assinaturas digitais e troca de chaves em SSL/TLS.

ECC (Elliptic Curve Cryptography)

Desenvolvido na década de 1980 pelos matemáticos Neal Koblitz e Victor Miller, o ECC representa um avanço significativo na criptografia assimétrica, oferecendo segurança robusta com eficiência e flexibilidade. Ele utiliza propriedades matemáticas de curvas elípticas para oferecer segurança robusta com chaves menores em comparação a algoritmos tradicionais como RSA. Com tamanhos de chave significativamente reduzidos, ECC é eficiente em termos de processamento, proteção de conexões na web e ideal para dispositivos limitados, sendo amplamente utilizado em aplicações como SSL/TLS e criptografia de mensagens seguras, comumente tendo 256, 384 ou 521 bits.