**Universidade São Judas Tadeu**

**Sistemas Computacionais e Segurança**

**Prof° Robson Calvetti**

Lucas Gabriel Hora Benetti - 825134041

**1. Exemplos Históricos do Uso de Criptografia**

* **O Disco de Alberti (c. 1467):** Inventado pelo arquiteto e polímata italiano Leon Battista Alberti, este é considerado o primeiro exemplo de uma cifra polialfabética (onde uma letra do texto simples pode ser representada por diferentes letras cifradas, dependendo de sua posição). Foi um avanço significativo em relação às cifras monoalfabéticas (como a de César), pois tornava a criptoanálise muito mais difícil.
* **A Cifra ADFGX (Primeira Guerra Mundial):** Usada pelo exército alemão, era uma cifra de transposição combinada com uma cifra de substituição. Era um sistema bastante complexo e forte para a época. Seu nome deriva das únicas cinco letras usadas no texto cifrado: A, D, F, G, X (e, em uma versão posterior, Y), escolhidas porque são fáceis de distinguir ao serem transmitidas por código Morse.

**2. Algoritmos de Criptografia com Chaves Simétricas Atuais**

* **Blowfish:** Criado por Bruce Schneier, é um algoritmo rápido, livre de patentes, e usa chaves de 32 a 448 bits. É comumente usado em softwares de encriptação de arquivos e discos, como o TrueCrypt (embora sua segurança possa ser comprometida para chaves menores de 448 bits).
* **ChaCha20:** É uma cifra de fluxo, conhecida por sua alta performance em software. É frequentemente usado em conjunto com o Poly1305 (um código de autenticação) para formar o ChaCha20-Poly1305 (AEAD), que é a cifra recomendada para segurança de transporte na internet (TLS) em muitos casos, oferecendo uma alternativa rápida e segura ao AES em dispositivos móveis e sistemas com recursos limitados.

**3. Algoritmos de Criptografia com Chaves Assimétricas Atuais**

* **Diffie-Hellman (DH) Key Exchange:** Não é um algoritmo de criptografia para mensagens inteiras, mas sim um método essencial para que duas partes que nunca interagiram antes possam concordar secretamente sobre uma chave simétrica (segredo compartilhado) em um canal inseguro. Ele é fundamental para iniciar a maioria das comunicações seguras (como HTTPS/TLS).
* **Elliptic Curve Cryptography (ECC) - (Criptografia de Curva Elíptica):** É uma abordagem moderna que adapta algoritmos assimétricos como Diffie-Hellman e DSA (resultando em ECDH e ECDSA). A principal vantagem do ECC é que ele oferece o mesmo nível de segurança que o RSA, mas com chaves muito menores (por exemplo, uma chave ECC de 256 bits é tão segura quanto uma chave RSA de 3072 bits). Isso o torna ideal para dispositivos móveis e ambientes de baixa largura de banda.