Criptografias

Exercício Aula - 4

Davi Deosmar Batista Oliveira Miranda – RA: 823.212.282
Silas Rodrigues Nascimento – RA: 823.273.38

Histórias de Criptografias

Scytale

A cifragem com o scytale (bastão, em grego) ou cítala espartana consistia em se enrolar uma fita de tecido em um bastão de madeira de dada largura.

A frase a ser cifrada era escrita na fita no comprimento do bastão, desenrolada e enviada disfarçada (como um cinto por exemplo) e ao chegar ao destino deveria ser enrolada num bastão de mesma largura para que a mensagem fosse decifrada.

Também era conhecida como bastão de Licurgo, embora alguns estudiosos citam que este tipo de cifra não passa de um mito.

Edward Hebern

A máquina rotativa Hebern foi criada por Edward Hebern em Illinois em 1917. Esta máquina marcou a primeira vez que circuitos elétricos foram usados em um dispositivo de cifra, pois combinava as partes mecânicas de uma máquina de escrever padrão e as partes elétricas da máquina de escrever elétrica.

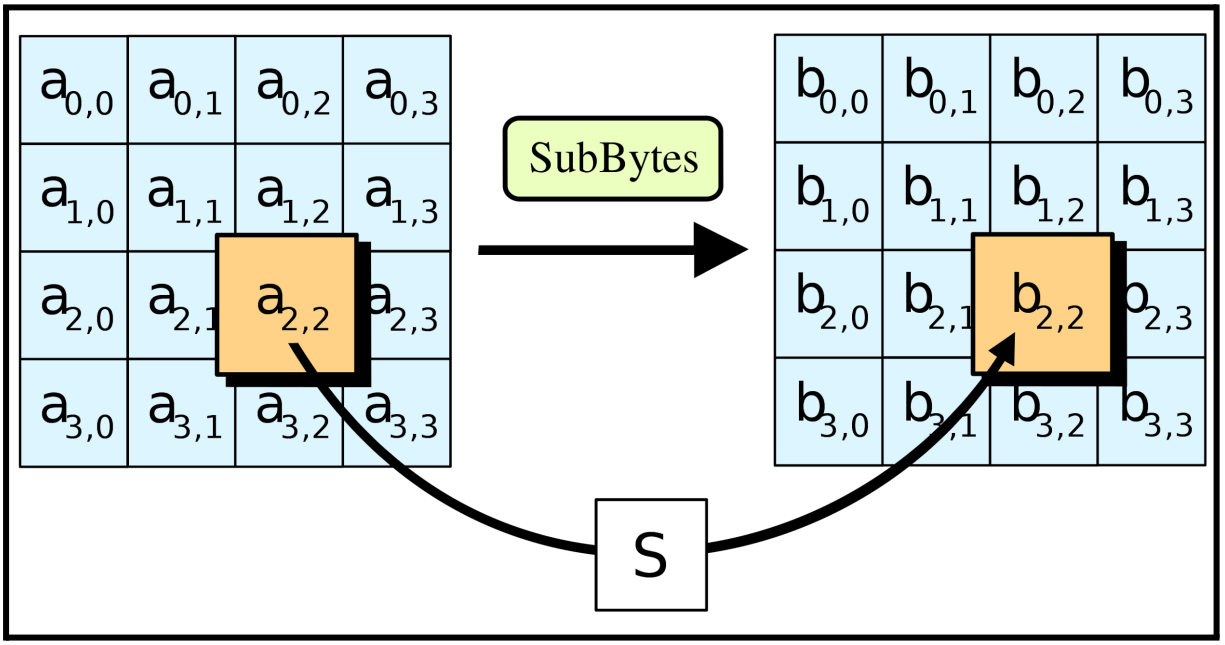
Conectada por meio de um misturador, a máquina incluía um disco com contatos elétricos em ambos os lados (também conhecido como rotor).

Fios foram usados para conectar cada letra a outra letra do lado oposto de maneira aleatória, também conhecida como alfabeto de substituição única.

Criptografias simétricas

A.E.S.

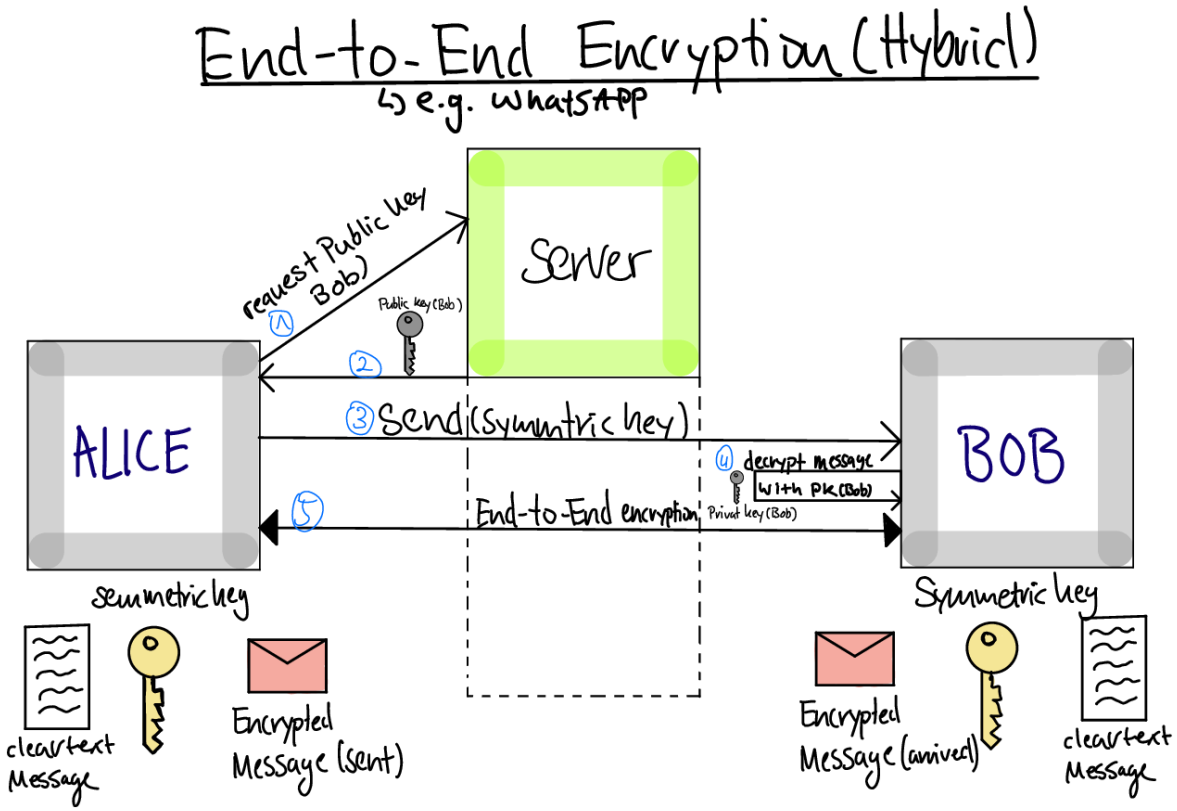
O AES é um subconjunto da cifra de bloco Rijndael desenvolvida por dois criptógrafos belgas, Vincent Rijmen e Joan Daemen, que submeteram uma proposta ao NIST durante o processo de seleção do AES. A Rijndael é uma família de cifras com diferentes tamanhos de chave e bloco. Para o AES, o NIST selecionou três membros da família Rijndael, cada um com um tamanho de bloco de 128 bits, mas três comprimentos de chave diferentes: 128, 192 e 256 bits.



O AES foi adotado pelo governo dos Estados Unidos da América. Ele substitui o padrão de criptografia de dados (DES), que foi publicado em 1977. O algoritmo descrito pelo AES é um algoritmo de chave simétrica, o que significa que a mesma chave é usada para criptografar e descriptografar os dados

Twosfish

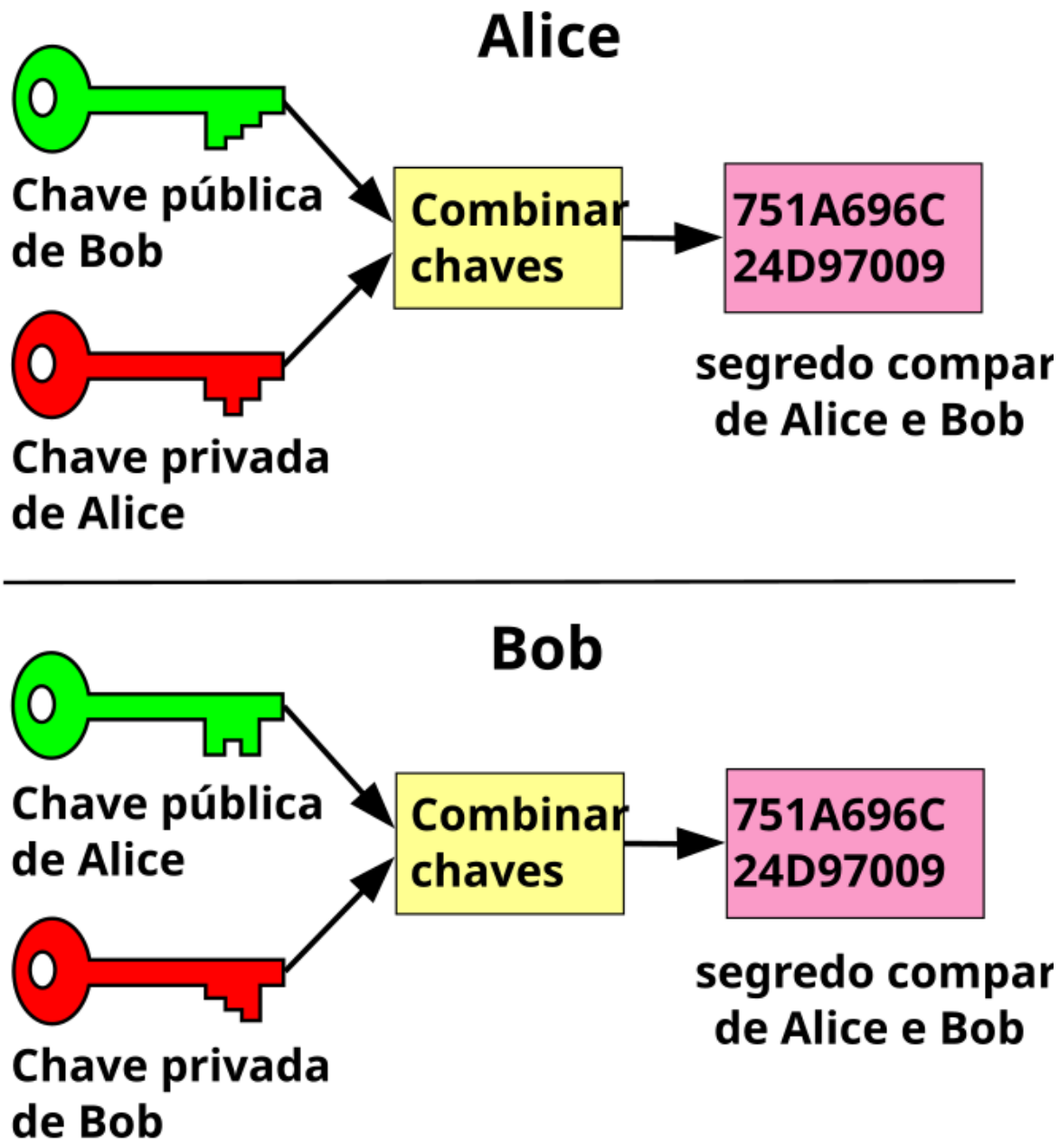
Twofish é um algoritmo de criptografia simétrica que utiliza uma única chave para criptografar e descriptografar dados e informações. Ele aceita a chave juntamente com as informações em texto simples . Essa chave então transforma as informações em texto cifrado , que não pode ser compreendido sem decodificação. Os dados criptografados são enviados ao destinatário junto com a chave de criptografia, após o texto cifrado ou junto com ele. O usuário pode usar essa chave para descriptografar as informações criptografadas.



Embora não seja considerado um padrão de criptografia avançado, o Twofish oferece uma alternativa mais eficiente e segura ao algoritmo DES . Um dos motivos é seu tamanho de bloco de 128 bits, o que o torna resistente a ataques de força bruta . Outro motivo é seu complexo agendamento de chaves com suporte para vários tamanhos de chaves.

Criptografias Assimétricas

Rivest–Shamir–Adleman (RSA)



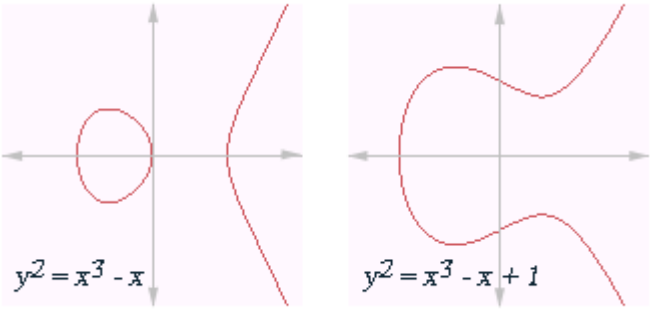
O Rivest–Shamir–Adleman (RSA) é um exemplo de algoritmo de criptografia assimétrica utilizado nos protocolos de segurança da internet (SSL e TLS), serviços de e-mails e acesso seguro a servidores e outros dispositivos computacionais por meio do protocolo SSH.

O RSA se baseia, matematicamente, na dificuldade de fatorar o produto de dois números primos com vários dígitos (por exemplo, acima de 100).

Quanto maior o número de dígitos, mais complexo e difícil será o processo de quebra da criptografia, um procedimento computacional que demandaria dezenas de anos de tentativas e erros.

Quando você acessa um site com [“https://”] e vê um cadeado verde na barra de endereço do navegador, isso indica que a comunicação entre o seu navegador e o servidor web está protegida usando um algoritmo de criptografia assimétrica.

Curvas Elípticas



A Criptografia de Curvas Elípticas, é uma aproximação para a criptografia de chave pública com base na estrutura algébrica de curvas elípticas sobre corpos finitos . A utilização de curvas elípticas em criptografia foi sugerida por Neal Koblitz e Victor S.Miller em 1985. Curvas Elípticas são também utilizadas em várias fatorações de algoritmos inteiros, que têm aplicações em criptografia.

Criptografia de chave pública é baseada na criação de enigmas matemáticos que são difíceis de resolver sem determinado conhecimento sobre como foram criados. O criador guarda aquele conhecimento secreto (a chave confidencial) e publicam o enigma (a chave pública). O enigma pode então ser usado para confundir uma mensagem de um jeito que somente o criador possa desconfundi-la. Antes, os sistemas de chaves públicas, tais como os algoritmos de RSA, usavam produtos de dois números primos como enigma: o usuário escolhe dois número primos como sua chave confidencial, e publica seu produto como sua chave pública. A dificuldade de fatoração assegura que ninguém mais possa desvendar a chave confidencial (isto é, os dois número primos) da chave pública. Entretanto, devido ao progresso recente em fatorar, chaves públicas de RSA devem agora ter milhares de bits de comprimento para fornecer a segurança adequada.