1.Conceitos fundamentais de criptografia

1.1 Cifras

Algoritmo matemático que realiza a transformação dos dados em formato legível (***texto claro***) para uma forma ilegível (***texto cifrado***) e vice-versa. A cifra utiliza a chave de criptografia como parâmetro para determinar como os dados serão embaralhados ou substituídos durante o processo de criptografia. É importante mencionar que diferentes cifras podem ser utilizadas na criptografia simétrica, como o algoritmo DES, AES, RC4, entre outros.

Nas **cifras de transposição**, nenhuma carta é substituída; elas são simplesmente reorganizadas. Os algoritmos de criptografia de bloco de criptografia modernos, como AES e o legado 3DES, ainda usam a transposição como parte do algoritmo.

As **cifras de substituição** substituem uma letra para outra. Em sua forma mais simples, as cifras de substituição mantêm a frequência de letras da mensagem original. A cifra de César foi uma simples cifra de substituição. Porque a mensagem inteira dependeu da mesma mudança de chave única, a cifra César é referida como uma cifra de substituição monoalfabética. Também é bastante fácil de rachar. Por esta razão, as cifras polialfabéticas, como a cifra Vigenère, foram inventadas.

1.2 Criptografia e Criptoanálise

A criptologia é a ciência de criar e violar os códigos secretos. A criptologia combina duas disciplinas separadas:

- **Criptografia:** O desenvolvimento e uso de códigos
- **Criptoanálise:** A quebra desses códigos

Enquanto houver criptografia, houve criptoanálise. A criptoanálise é a prática e o estudo de determinar o significado de informações criptografadas (quebrando o código), sem acesso à chave secreta compartilhada. Isso também é conhecido como codebreaking. Vários métodos são usados na criptoanálise, como:

- **Método de força bruta:** O atacante tenta todas as principais teclas sabendo que, eventualmente, um deles funcionará.
- **Método de cifra:** O atacante tem o texto cifrado de várias mensagens criptografadas, mas nenhum conhecimento do texto simples subjacente.
- **Método de texto simples:** O atacante tem acesso ao texto cifrado de várias mensagens e sabe algo sobre o texto simples subjacente a esse texto cifrado.
- **Método Chosen-plaintext:** O atacante escolhe quais dados o dispositivo de criptografia criptografa e observa a saída do cifra de texto.

- **Método chosen-ciphertext:** O atacante pode escolher diferentes texto cifrado a descriptografos e tem acesso ao texto simples descriptografado.
- **Método Meet-in-the-Middle:** O atacante conhece uma parte do texto simples e do cifrado correspondente.

Há uma relação simbiótica entre as duas disciplinas porque cada uma faz a outra mais forte. Organizações Nacionais de Segurança empregam profissionais de ambas as disciplinas e colocá-las a trabalhar uns contra os outros.

A criptoanálise é frequentemente usada por governos em vigilância militar e diplomática, pelas empresas em testar a força dos procedimentos de segurança e por hackers maliciosos na exploração de fraquezas nos sites. Embora a criptoanálise seja frequentemente ligada a propósitos travessos, é realmente uma necessidade. É um fato irônico da criptografia que é impossível provar que qualquer algoritmo é seguro. Só pode ser provado que não é vulnerável a ataques criptanalíticos conhecidos. Portanto, há necessidade de matemáticos, estudiosos e especialistas em segurança para continuar tentando quebrar os métodos de criptografia.

No mundo das comunicações e *networking,* autenticação, integridade e confidencialidade de dados são implementados de várias maneiras usando vários protocolos e algoritmos. A escolha do protocolo e do algoritmo varia com base no nível de segurança necessária para atender às metas da política de segurança da rede.

A escolha varia dependendo dos requisitos de segurança especificados no documento de política de segurança de rede. Considerações adicionais são o poder de computação que é necessário para criptografar e descriptografar dados e a aceitação do protocolo na comunidade de segurança.

2.Gerenciamento de chaves

O **gerenciamento de chaves** é frequentemente considerado a parte mais difícil do projeto de um criptosistema. Muitos criptossistemas falharam devido a erros de gerenciamento de chave e todos os algoritmos de criptografia modernos procedimentos de gerenciamento de chaves. Na prática, a maioria dos ataques a sistemas criptográficos são direcionados ao nível de gerenciamento de chaves, e não ao algoritmo criptográfico em si.

Característica	Descrição
Geração da chave	Era César quem escolhia a chave da cifra. Em um sistema criptográfico moderno, a geração da chave é geralmente automatizada e não é controlada pelo usuário final. O uso de geradores de número aleatórios eficientes é necessário para garantir que todas as chaves sejam igualmente geradas, de modo que o invasor não possa prever quais chaves têm maior probabilidade de serem usadas

Verificação da chave	Algumas chaves são melhores que outras. Quase todos os algoritmos criptográficos têm algumas chaves fracas que não devem ser usadas. Com a ajuda dos procedimentos de verificação de chave, as chaves fracas podem ser identificadas e regeneradas para proporcionar uma criptografia mais segura. Com a cifra de César, usar uma chave 0 ou 25 não criptografa a mensagem, portanto ela não deve ser usada
Troca de chave	Os procedimentos de gerenciamento de chave devem oferecer um mecanismo de troca de chaves confiável, que permita que as partes estabeleçam o material da chave com segurança, provavelmente usando um meio não confiável
Armazenamento de chave	Em um sistema operacional moderno de vários usuários que utiliza a criptografia, uma chave pode ser armazenada na memória. Isso representa um problema potencial, quando a memória é colocada no disco, porque um programa Cavalo de Troia instalado no PC de um usuário poderia ter acesso às chaves privadas dele
Duração da chave	O uso de curta duração da chave melhora a segurança das cifras antigas que são usadas em conexões de alta velocidade. Em IPsec, uma duração de 24 horas é típica. No entanto, alterar a duração para 30 melhora a segurança dos algoritmos
Revogação e destruição da chave	A revogação notifica todas as partes interessados que determinada chave foi comprometida e não deve mais ser usada. A destruição apaga chaves antigas de modo que evite a recuperação por invasores mal-intencionados

Dois termos usados para descrever as chaves são o **comprimento da chave** e o ***keyspace***.

2.1 Comprimento da chave

Também chamado de tamanho da chave, é a medida em bits. Neste curso, usaremos o termo comprimento da chave.

2.2 Keyspace

Este é o número de possibilidades que podem ser geradas por um comprimento de chave específico.

O espaço da chave de um algoritmo é o conjunto de todos os valores de chave possíveis. Uma chave que tem ***n*** bits produz um keyspace que tem 2^n valores-chave possíveis. Ao adicionar um pouco à chave, o ***keyspace*** é efetivamente duplicado.

Ao adicionar um bit ao comprimento da chave, o espaço de tecla dobra, e um atacante precisa do dobro de tempo para pesquisar o espaço de tecla. **Chaves mais longas são mais seguras**; no entanto, eles também consomem mais recursos. Deve-se ter cuidado ao escolher chaves mais longas, pois lidar com elas pode adicionar uma carga implicar ao processador em produtos da extremidade inferior.

Quase todo algoritmo tem algumas chaves fracas em seu ***keyspace*** que permitem a um invasor quebrar a criptografia por meio de um atalho. Chaves fracas mostram as regularidades na criptografia.

Vários tipos de chaves criptográficas podem ser gerados:

- **Chaves simétricas:** Pode ser trocado entre dois roteadores que suportam uma VPN
- **Chaves assimétricas:** São usados em aplicações HTTPS seguras
- **Chaves hash:** São usados em geração de chaves simétricas e assimétricas, assinaturas digitais e outros tipos de aplicações
- **Assinaturas digitais:** São usados quando se conecta a um site seguro

Independentemente do tipo de chave, todas as chaves compartilham problemas semelhantes. Escolher um comprimento de chave adequado é um problema. Se o sistema criptográfico for confiável, a única maneira de quebrá-lo é com um ataque de força bruta. Se o keyspace for grande o suficiente, a busca requer uma quantidade enorme de tempo, tornando um esforço tão exaustivo impraticável.

A tabela resume o comprimento da chave necessária para proteger os dados pelo período de tempo indicado.

Comprimento da proteção	Chave simétrica	Chave assimétrica	Assinatura digital	Hash
3 anos	80	1248	160	160
10 anos	96	1776	192	192
20 anos	112	2432	224	224
30 anos	128	3248	256	256
Proteção contra computadores quânticos	256	15424	512	512

Em média, um invasor tem que pesquisar **a metade do espaço chave antes que a chave correta seja encontrada**. O tempo necessário para realizar essa pesquisa depende da potência do computador disponível para o atacante. Os comprimentos de chave atuais podem facilmente tornar qualquer tentativa insignificante porque leva milhões ou bilhões de anos para concluir a pesquisa quando uma chave suficientemente longa é usada.

O desempenho é outro problema que pode influenciar a escolha de um comprimento chave. Um administrador deve encontrar um bom equilíbrio entre a velocidade e a força de proteção de um algoritmo, porque alguns algoritmos, como o algoritmo Rivest, Shamir e Adleman (RSA), são executados lentamente devido a grandes comprimentos de chave.

Devido aos rápidos avanços na tecnologia e métodos criptanalíticos, o comprimento chave que é necessário para uma determinada aplicação está aumentando constantemente. Parte da força do algoritmo RSA é a dificuldade de fatoração de grandes números.

3.WEP

Wired Equivalent Privacy é um protocolo de segurança que tentou fornecer uma WLAN com o mesmo nível de segurança de uma LAN com fio. Como as medidas de seguranças físicas ajudam a proteger uma LAN com fio, o WEP procura fornecer proteção similar para dados transmitidos pela WLAN com criptografia. O WEP usa uma chave de criptografia, porém, não há provisão para gerenciamento de tecla com WEP, então o número de pessoas que compartilham a chave continuará a crescer. Ele também tem vários problemas com o seu vetor de inicialização, que é um dos componentes do sistema criptográfico.

4.WPA

Wi-Fi Protected Access surgiu como um protocolo melhorado para substituir o WEP. O WPA2 não tem os mesmos problemas de criptografia, pois um invasor não pode recuperar a chave pela observação do tráfego. O WPA2 está suscetível ao ataque porque criminosos virtuais podem analisar os pacotes transmitidos entre o access point e um usuário legítimo.