INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Arquitetura de Redes de Computadores
Atividade 20: Introdução a Criptografia e Criptoanálise

Utilizar a Internet requer que alguns cuidados sejam tomados e, para isto, é importante que você esteja informado dos riscos aos quais está exposto. Alguns destes riscos são:

- Acesso a conteúdos impróprios ou ofensivos: pode se deparar com páginas que contenham crimes, que atentem contra a honra ou que incitem o ódio e o racismo.
- Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.
- Furto e perda de dados: os dados presentes em seus equipamentos conectados a Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.
- Divulgação de boatos: pessoas podem usar a Internet para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.
- Dificuldade de exclusão: aquilo que e divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você.

Criptografia

Uma maneira de tentar minimizar os riscos na Internet é utilizando técnicas que visam garantir a confidencialidade dos dados. Criptografia é o conjunto de técnicas utilizadas para proteger informações, transformando dados legíveis (texto simples) em dados embaralhados (texto cifrado), de forma que apenas pessoas autorizadas consigam entendê-los.

Esse processo utiliza algoritmos matemáticos e chaves criptográficas para garantir a confidencialidade das informações durante o armazenamento ou a transmissão de dados.

A confidencialidade significa que somente o remetente e o destinatário devem poder "entender" o conteúdo da mensagem transmitida. A mensagem original, antes de ser transformada, é chamada texto claro. Após transformada, ela é denominada simplesmente texto cifrado. Um algoritmo de criptografia transforma o texto claro em texto cifrado; um algoritmo de decriptografia transforma o texto cifrado de volta para texto claro. O emissor usa um algoritmo de criptografia e o receptor utiliza um algoritmo de decriptografia.

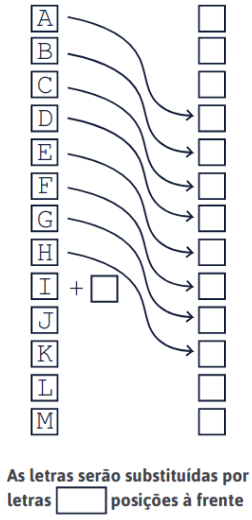
Ela é utilizada há milênios e que atualmente faz parte do nosso cotidiano oferecendo soluções eficazes no que diz respeito à segurança da informação. Ela é uma ferramenta de segurança amplamente utilizada nos meios de comunicação e consiste basicamente na transformação de determinado informação a fim de ocultar seu real significado. Só quem souber o algoritmo e tiver a chave certa poderá reverter a mensagem cifrada para o conteúdo original.

A criptografia é essencial no mundo digital porque protege senhas, dados bancários e informações pessoais, garantindo a segurança das transações realizadas pela internet. Ela também evita o roubo de dados e a prática de espionagem digital, além de proteger as comunicações em redes públicas, que são mais vulneráveis a ataques.

Cifra de César

A Cifra de César, também conhecida como cifra de troca, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes. Por exemplo, com uma troca de três posições, A seria substituído por D, B se tornaria E, e assim por diante. O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.

A transformação pode ser representada alinhando-se dois alfabetos; o alfabeto cifrado é o alfabeto normal rotacionado à direita ou esquerda por um número de posições. Por exemplo, aqui está uma cifra de César usando uma rotação à esquerda de três posições (o parâmetro de troca, três neste caso, é usado como chave).




```
Normal:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado: DEFGHIJKLMNOPQRSTUVWXYZABC
```

Para criptografar uma mensagem, deve-se simplesmente observar cada letra da mensagem na linha “Normal” e escrever a letra correspondente na linha “Cifrado”. Para descriptografar, deve-se fazer o contrário.

```
Normal:  voce ganhou um ponto
Cifrado: yrfh jdqkrx xp srqwr
```

Atualmente, A cifra de César é utilizada para fins didáticos pois ela pode ser facilmente decifrada usando as mesmas técnicas usadas análise de frequência ou verificando os padrões de palavras. Por exemplo, uma vez que existe apenas um número limitado de rotações possíveis (26 em português, se desconsiderarmos o uso de cedilha e letras acentuadas), cada uma pode ser testada por turno num ataque de força bruta, ou se for um texto grande, tentar observar as letras que mais se repetem (na língua portuguesa seria a letra ”a”, ”e”, ”o” e ”s”, por exemplo, são as quatro mais utilizadas na nossa língua).

Criptoanálise

A criptoanálise pode ser definida como o conjunto de métodos e estratégias empregadas para analisar e comprometer sistemas criptográficos, explorando falhas matemáticas, lógicas ou de implementação. O criptoanalista tenta recuperar a mensagem original, a chave secreta ou informações parciais sem autorização.

Os principais tipos de ataques criptoanalíticos incluem:

- Ataque de Força Bruta: consiste em testar todas as chaves possíveis até encontrar a correta. É simples, porém exige alto poder computacional para chaves complexas.
- Ataque por Texto Conhecido: o atacante possui partes da mensagem original e do texto cifrado, utilizando essas informações para descobrir a chave.
- Ataque por Texto Escolhido: o atacante escolhe mensagens específicas para serem criptografadas e analisa os resultados para identificar padrões no algoritmo.
- Ataque Estatístico: explora padrões de frequência de letras e símbolos, muito comum em cifras clássicas como a Cifra de César.

Atividade

1. Forme grupos (até 4 componentes). Cada grupo irá criar uma mensagem secreta, usando a cifra de César, com no mínimo 15 e no máximo 30 caracteres. Depois de que todos os grupos crirem, colocar no quadro.

2. Quando todas as mensagens estiverem no quadro, os grupos irão tentar decifrar os códigos secretos dos outros grupos. O grupo vencedor será o que conseguir decifrar o maior número de códigos.