Atividade 2 - Técnicas de Encriptação
Aluno: João Victor Póvoa França

REVISÃO

2.1 Quais são os elementos essenciais de uma cifra simétrica?

Um esquema de encriptação simétrica possui cinco ingredientes: texto claro (a mensagem original), algoritmo de encriptação, chave secreta, texto cifrado (a mensagem embaralhada) e algoritmo de decriptação.

2.2 Quais são as duas funções básicas usadas nos algoritmos de encriptação?

Todos os algoritmos de encriptação são baseados em dois princípios gerais: substituição (onde cada elemento do texto claro é mapeado em outro elemento) e transposição (onde os elementos do texto claro são rearranjados).

2.3 Quantas chaves são necessárias para duas pessoas se comunicarem por meio de uma cifra?

Se o sistema for de encriptação simétrica (cifra convencional), é necessária apenas uma chave secreta, que é compartilhada tanto pelo emissor quanto pelo receptor. Se o sistema for de encriptação assimétrica (chave pública), são usadas duas chaves diferentes.

2.4 Qual é a diferença entre uma cifra de bloco e uma cifra de fluxo?

Uma cifra de bloco processa a entrada um bloco de elementos de cada vez, produzindo um bloco de saída para cada bloco de entrada correspondente. Já uma cifra de fluxo processa os elementos da entrada de forma contínua, proporcionando a saída de um elemento por vez.

2.5 Quais são as duas técnicas gerais para atacar uma cifra?

As duas técnicas gerais são a criptoanálise e o ataque por força bruta.

2.6 Liste e defina rapidamente os tipos de ataque criptoanalítico com base naquilo que o atacante conhece.

Apenas texto cifrado: O criptoanalista conhece apenas o algoritmo de encriptação e o texto cifrado.
Texto claro conhecido: O atacante tem o algoritmo, o texto cifrado e um ou mais pares de texto claro-texto cifrado produzidos pela chave secreta.
Texto claro escolhido: O atacante conhece o algoritmo, o texto cifrado e uma mensagem de

texto claro que ele mesmo escolheu, com seu respectivo texto cifrado gerado com a chave.
Texto cifrado escolhido: Conhece o algoritmo, o texto cifrado e um texto cifrado escolhido pelo atacante, juntamente com seu respectivo texto claro decriptado.
Texto escolhido: Combina o acesso tanto a textos claros escolhidos quanto a textos cifrados escolhidos, juntamente com seus respectivos pares gerados.

2.7 Qual é a diferença entre uma cifra incondicionalmente segura e uma cifra computacionalmente segura?
Um esquema é incondicionalmente seguro se o texto cifrado gerado por ele não tiver informações suficientes para determinar exclusivamente o texto claro correspondente, não importando a quantidade de texto cifrado ou de tempo à disposição do atacante. Um esquema é considerado computacionalmente seguro se o custo para quebrar a cifra ultrapassar o valor da informação protegida, ou se o tempo exigido para quebrá-la superar o tempo de vida útil da informação.

2.8 Defina resumidamente a cifra de César.
É a cifra de substituição mais antiga e simples, que envolve substituir cada letra do alfabeto por aquela que fica três posições adiante (ou qualquer deslocamento fixo de magnitude k) de forma rotativa.

2.9 Defina resumidamente a cifra monoalfabética.
É uma técnica de substituição na qual um único alfabeto de cifra (uma permutação que mapeia do alfabeto claro para um cifrado) é utilizado para criptografar toda a mensagem.

2.10 Defina resumidamente a cifra Playfair.
É uma cifra de substituição de múltiplas letras que trata os digramas (pares de letras) no texto claro como unidades isoladas e as traduz para digramas de texto cifrado, baseando-se no uso de uma matriz 5x5 de letras construída a partir de uma palavra-chave.

2.11 Qual é a diferença entre uma cifra monoalfabética e uma polialfabética?
Enquanto a cifra monoalfabética utiliza sempre o mesmo alfabeto de substituição para a mensagem inteira, a cifra polialfabética usa um conjunto de diferentes regras de substituição monoalfabéticas à medida que prossegue pela mensagem, sendo a escolha da regra definida por uma chave.

2.12 Quais são os dois problemas com o one-time pad?

1. O problema prático de se criar grandes quantidades de chaves verdadeiramente aleatórias, exigindo milhões de caracteres aleatórios regularmente.
2. O gigantesco problema de distribuição e proteção das chaves, visto que para cada mensagem enviada, uma chave aleatória de igual tamanho e de uso único precisa ser entregue de forma segura tanto para o emissor quanto para o receptor.

2.13 O que é uma cifra de transposição?
É uma técnica de criptografia onde nenhum elemento do texto claro é alterado, mas sim os elementos sofrem algum tipo de permutação ou rearranjo de suas posições na mensagem (como, por exemplo, escrever os caracteres em colunas e lê-los em diagonais).

2.14 O que é esteganografia?
Ao contrário das cifras que ocultam o significado da mensagem, a esteganografia é uma técnica utilizada para ocultar a própria existência da mensagem (como, por exemplo, o uso de tinta invisível).

PROBLEMAS

Problema 2.5: A Cifra de Livro (Ruth Rendell)

a. Qual é o algoritmo de encriptação?

O algoritmo é uma cifra de substituição monoalfabética simples. A chave do alfabeto cifrado é construída utilizando as letras únicas da primeira frase do livro na ordem em que aparecem.

Na frase *"The snow lay thick on the steps..."*, extraindo apenas as letras inéditas da esquerda para a direita, obtemos a sequência: T, H, E, S, N, O, W, L, A, Y, I, C, K, P, D, F, R, V, B, G.

Assim, a letra 'A' do texto claro vira 'T' no cifrado; o 'B' vira 'H'; o 'C' vira 'E', o 'D' vira 'S' e assim por diante. Quando o texto cifrado SIDKHKDM é submetido ao processo inverso (S->b, I->a, D->s, K->i, H->l, K->i, D->s, M->k), ele revela a palavra "basilisk".

b. Qual a sua segurança?

A segurança é muito fraca. Como cada letra do alfabeto original é sempre mapeada para a

mesma letra no texto cifrado, a cifra retém todas as propriedades estatísticas (frequências de letras e padrões de palavras) do idioma original, tornando-a facilmente quebrável por criptoanálise de frequência básica.

c. Por que usar a primeira sentença é preferível à última?

A primeira sentença do primeiro capítulo de um livro é inambígua e fácil de localizar rapidamente. A "última sentença" de um livro pode ser ambígua dependendo da edição (pode haver posfácios, apêndices, notas do autor ou índices). Além disso, do ponto de vista prático de espionagem e segurança, procurar a última frase exige folhear o livro até o fim, correndo o risco de acidentalmente ler *spoilers* da história ou chamar atenção indevida.

Problema 2.6: O Código de Sherlock Holmes

Sherlock Holmes deduziu tratar-se de uma Cifra de Livro (Book Cipher) clássica, também conhecida como cifra de dicionário ou almanaque.

Na mensagem, 534 representa o número da página de um livro pré-combinado entre as partes, e C2 refere-se à Coluna 2 dessa página. Os números subsequentes (13, 127, 36...) são as posições exatas das palavras contando do topo daquela coluna. Palavras que o emissor não conseguiu encontrar na referida página do livro (como nomes próprios: "DOUGLAS" e "BIRLSTONE") foram escritas abertamente em texto claro para não travar a comunicação.

Problema 2.7: Manual das Forças Especiais

a. Encriptação (Transposição Dupla):

O manual utiliza uma Cifra de Transposição Colunar Dupla. O texto é escrito em uma grade da esquerda para a direita e as colunas são lidas com base na ordem alfabética da palavra-chave.

- **Suposições razoáveis: Removemos espaços e pontuação; letras redundantes nas chaves recebem numeração da esquerda para a direita; e preenchemos os espaços vazios da grade final com 'X' para disfarçar o tamanho da mensagem.**
- **Passo 1: Usando a chave CRYPTOGRAPHIC (13 colunas), escrevemos o texto em linhas. A ordem de leitura das colunas será determinada pela ordem alfabética da palavra (C=1, C=2, G=3...).**
- **Passo 2: O texto resultante do primeiro embaralhamento é inserido em uma nova**

matriz governada pela chave NETWORK SECURITY (15 colunas), lendo as colunas novamente na nova ordem alfabética para gerar o texto cifrado final.

b. Decriptação:

Para decriptar, o receptor faz exatamente a engenharia reversa. O texto cifrado é dividido em colunas baseando-se no tamanho da chave NETWORK SECURITY e reconstruído linha por linha. Esse resultado é novamente colocado em colunas baseadas em CRYPTOGRAPHIC para recuperar o texto claro ("*Be at the third pillar...*").

c. Apropriabilidade e vantagens:

Esta técnica é extremamente apropriada para operações táticas em campo (Forças Especiais).

- **Vantagens: Não exige nenhum tipo de equipamento eletrônico, computador ou máquina de rotores — apenas caneta, papel e a memorização de duas senhas. Apesar de manual, a transposição dupla destrói os diagramas normais da linguagem de forma muito eficiente, oferecendo uma segurança altíssima contra criptoanalistas se for interceptada.**

Problema 2.9: O Incidente do PT-109

Cifra Playfair

A palavra-chave é "royal new zealand navy". Extraindo as letras não repetidas, obtemos a chave base: R O Y A L N E W Z D V. Colocamos isso em uma matriz 5x5 (lembrando que I e J dividem o mesmo espaço).

A matriz final fica assim:

R O Y A L

N E W Z D

V B C F G

H I K M P

Q S T U X

O texto cifrado recebido foi:

KX JE YU RE BE ZW EH EW RY TU HE YF SK RE HE GO YF IW TT TU OL KS YC AJ PO BO TE IZ ON TX BY BN TG ON EY CU ZW RG DS ON SX BO UY WR HE BA AH YU SE DQ

Agrupando e decriptando pelos pares da Playfair (e traduzindo a anomalia "TT" diretamente para "tt", conforme exigido pelo exercício), temos:

- **KX $\rightarrow$ PT**
- **JE $\rightarrow$ BO**
- **YU $\rightarrow$ AT**
- **RE $\rightarrow$ ON**
- **BE $\rightarrow$ EO**
- **ZW $\rightarrow$ WE**
- **EH $\rightarrow$ NI**
- **EW $\rightarrow$ NE**
- **RY $\rightarrow$ LO**
- **TU $\rightarrow$ ST**
- ***(...e assim por diante para todo o bloco)***

Mensagem Decriptada Final:

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKEtt STRAIT TWO MILES SW MEREUS COVE X CREW OF TWELVE X REQUEST ANY INFORMATION X

(Tradução livre contextual: O Barco PT 109 foi perdido em ação no Estreito de Blackett, duas milhas a sudoeste da enseada de Mereus [Merkus]. Tripulação de doze. Solicito qualquer informação).