Relatório do Laboratório 1
Segurança de Dados - Professora Denise Goya

Luiz Ricardo Bitencourt

25/02/2024

1 Implementação da Cifra de Vigenère

O laboratório propôs a criação de um programa para simular a Cifra de Vigenère, com duas funcionalidades: cifrar e decifrar. Abaixo, apresento os métodos criados para estas funcionalidades, mas o código completo pode ser conferido anexo.

Método para cifrar:

```
void encrypt(char key[], char originalMessage[], char encryptedMessage[], int size){
    if (DEBUG) printf("Encrypted message (inside function): ");
    for (int i = 0; i < size; i++) {
        encryptedMessage[i] = ((((originalMessage[i] - OFFSET) + (key[i % KEY_SIZE]) - OFFSET)) % ALPHABET_SIZE) + OFFSET;
        if (DEBUG) printf("%c", encryptedMessage[i]);
    }
    if (DEBUG) printf("\n\n");
}
```

Método para decifrar:

```
void decrypt(char key[], char mEncrypted[], char mDecrypted[], int size){
    int i;
    if (DEBUG) printf("Decrypted message (inside function): ");
    for (i = 0; i < size; i++) {
        mDecrypted[i] = (((mEncrypted[i] - OFFSET) - (key[i % KEY_SIZE] - OFFSET) + ALPHABET_SIZE) % ALPHABET_SIZE) + OFFSET;
        if (DEBUG) printf("%c", mDecrypted[i]);
    }
```

```
8       if (DEBUG) printf("\n\n");
9   }
```

2 Sobre a vulnerabilidade

Para este laboratório, foi sugerido responder ao questionamento: **por que a expressão algébrica equivale ao uso da Tabela de Vigenère com lápis e papel?** Analisando-se o processo de cifragem, é possível construir uma tabela com as palavras nas colunas e a chave nas linhas, realizando-se um cruzamento a cada novo caractere de forma a gerar, manualmente, a mensagem cifrada. Algebricamente, nota-se que cada caractere cifrado é a soma do índice do caractere da mensagem com o seu correspondente à chave, dentro do intervalo de caracteres do alfabeto utilizado. Por isso a tabela acaba sendo um recurso facilitador na cifragem. O processo inverso também é possível de maneira semelhante, porém montando uma tabela que considera a subtração do índice do caractere ao índice da chave, somando-se o tamanho do alfabeto e relacionando o valor obtido a este. A título de curiosidade, foi feito o processo de cifragem da palavra "universidade" usando a chave "abc" pelo cruzamento em uma tabela, conforme Figura 1, e também usando os índices da tabela para a cifragem e decifragem manual usando diretamente a expressão algébrica, conforme Figura 2.

		PALAVRA																						
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
		a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**x**	**z**
CHAVE	0 **a**	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	z
	1 **b**	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	z	a
	2 **c**	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	z	a	b

Cifra pelo cruzamento na tabela:												
Palavra:	u	n	i	v	e	r	s	i	d	a	d	e
Chave:	a	b	c	a	b	c	a	b	c	a	b	c
Cifrado:	u	o	k	v	f	t	s	j	f	a	e	g

Figura 1: Cifragem pela tabela.

Crifra pela expressão algébrica Ci = (Mi + Ki)mod(23):												
Índice Mi:	20	13	8	21	4	17	18	8	3	0	3	4
Índice Ki:	0	1	2	0	1	2	0	1	2	0	1	2
Mi + Ki:	20	14	10	21	5	19	18	9	5	0	4	6
Ci:	20	14	10	21	5	19	18	9	5	0	4	6
Cifrado:	**u**	**o**	**k**	**v**	**f**	**t**	**s**	**j**	**f**	**a**	**e**	**g**

Decifra pela expressão algébrica Mi = (Ci - Ki + 23)mod(23):												
Índice Ci:	20	14	10	21	5	19	18	9	5	0	4	6
Índice Ki:	0	1	2	0	1	2	0	1	2	0	1	2
Ci - Ki + 23:	43	36	31	44	27	40	41	31	26	23	26	27
Mi:	20	13	8	21	4	17	18	8	3	0	3	4
Decifrado:	**u**	**n**	**i**	**v**	**e**	**r**	**s**	**i**	**d**	**a**	**d**	**e**

Figura 2: Cifragem pela expressão algébrica.

A Cifra de Vigenère é uma versão melhorada da Cifra de César, baseada na substituição de caracteres. Esta última é baseada na adoção de uma tabela de substituição, da qual se extraem informações sobre qual caractere deve ser usado para substituir cada caractere da mensagem original. Isso

significa que pode-se chegar a mensagem original realizando-se uma análise da frequência de caracteres, seus posicionamentos, início e final de frases, etc. Tudo isso poderia ser usado para dar indícios de quais seriam as substituições, tornando a cifra vulnerável. Já a cifra de Vigenère usa uma tabela de substituição que varia a cada caractere, sendo uma cifra polialfabética que usa uma chave secreta para realização das combinações e geração da mensagem cifrada. Apesar de ser mais difícil de ser quebrada, já que a análise de frequência de caracteres não tem mais validade, como se tem uma mesma chave podem ocorrer repetições dos padrões em intervalos regulares, o que pode dar indícios do tamanho da chave. De posse dessa informação, é possível descobrir trechos da chave, o que possibilita decifrar trechos da informação e, iterativamente, toda a mensagem.