FACULDADE DE TECNOLOGIA, CIÊNCIAS E EDUCAÇÃO

Graduação

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Segurança da Informação em Organizações Empresariais: o uso da Criptoanálise para testar algoritmos de encriptação

Lydianne Tenório Intra
Lívia Castro Degrossi (Orientadora)

RESUMO

A informação possui significativa importância, visto que o diferencial das empresas está diretamente ligado à valorização que dão à informação, auxiliando no processo decisório e a explorar oportunidades de investimento. Sabendo disso, crackers pelo mundo inteiro tentam roubar essas informações através de ataques cibernéticos (ação praticada por crackers que consiste em roubar informações e comprometer o funcionamento de computadores ou rede de dados) a fim obter vantagens ilícitas e causar danos. A aplicação de um algoritmo de encriptação seguro é de fundamental importância para a empresa, pois impede indivíduos mal-intencionados de obter acesso a informações sigilosas. O objetivo deste trabalho é utilizar a criptoanálise para testar a segurança dos algoritmos selecionados e fazer uma análise comparativa entre eles, a fim de auxiliar na garantia da Confidencialidade, Integridade e Disponibilidade dos dados e minimizar potenciais ataques. Trata-se de uma pesquisa a qual apontou os tipos de ataques sobre mensagens encriptadas, o conceito de criptografia de dados, e como a criptoanálise pode ajudar na escolha de algoritmos mais eficientes. Apresentou ainda os resultados das técnicas capazes de “quebrar” as cifras utilizadas, de modo a obter o texto original, a implementação em linguagem C das cifras utilizadas e um comparativo entre os algoritmos de encriptação selecionados.

Palavras-chaves: Segurança da informação. Criptografia. Rede de dados. Criptoanálise. Algoritmos de encriptação.

ABSTRACT

Information is significantly important to organizations, since provides value to them, aids in the decision making process and explores investment opportunities. On this basis, crackers around the world try to steal information by means of cyber attacks, actions that involves stealing information and compromising the work of computers or data networks, in order to gain illicit benefits and harm. The application of a secure encryption algorithm is important to companies as it prevents malicious individuals from gaining access to sensitive information. The purpose of this work is to use cryptoanalysis to test the security of two algorithms and make a comparative analysis between them in order to guarantee Confidentiality, Integrity and Availability of a dataset and to minimize potential attacks. In this work, it is pointed out the types of attacks on encrypted messages, the concept of data encryption, how cryptanalysis can help choosing more efficient algorithms and a comparison between the selected encryption algorithms. It also presents the results of two techniques capable of "breaking" texts. The algorithms were implemented in C language.

Keywords: Information security. Cryptography. Data Network. Cryptanalysis. Encryption algorithms.

Introdução

A informação tornou-se o principal ativo das organizações empresariais e é de fundamental importância para que estas alcancem vantagem competitiva (LYRA, 2008, p. 5): “As ameaças ao principal ativo organizacional, isto é, à informação, aumentam a cada dia. Portanto, como a informação é a base da vantagem competitiva de uma organização, é vital garantir a segurança dessa informação”.

O avanço da tecnologia trouxe consigo numerosos benefícios. Contudo, a disseminação de novas tecnologias e o crescente número de pessoas envolvidas com a programação colaboraram com o aumento dos desafios para combater as novas ameaças e ataques que surgem. Conforme o jornal internacional El País do dia 27 de junho de 2017, a estatal russa Rosneft, do setor petrolífero, a multinacional dinamarquesa Moller-Maersk, a farmacêutica MSD, a holding britânica WPP e setores do governo da Ucrânia e Espanha foram vítimas de um ciberataque Ransomware, um sequestro de dados, baseado em uma tecnologia roubada da Agência de Segurança Nacional dos EUA. O Ransomware costuma se espalhar com o simples gesto de abrir um e-mail ou um arquivo anexado ou na instalação de um programa no computador. Operações e transações em

dezenas de bancos na Ucrânia foram interrompidas pelo ciberataque. Os hackers pediram o pagamento de 300 dólares por meio do bitcoin para não vazarem informações das empresas afetadas pelo ciberataque. Neste contexto, as empresas estão buscando proteger seus dados e utilizar mecanismos de segurança eficazes e atualizados como, por exemplo, o uso de assinaturas digitais, o que torna possível assinar documentos digitalmente garantindo autenticidade e integridade ao documento, por utilizar algoritmos de criptografia juntamente com funções unidirecionais ou hash criptográficas. Uma função hash, também conhecida como função de resumo, é uma equação matemática que a partir de um texto gera uma cadeia de caracteres de tamanho fixo, podendo ser comparado a uma impressão digital, pois cada documento possui um valor único de resumo, e qualquer alteração no documento resulta em uma hash completamente diferente (XAVIER; MENDES; MONTEIRO, 2015). E é neste contexto que verifica-se a importância da criptografia em uma rede de dados.

O objetivo deste trabalho é utilizar a criptoanálise para verificar diferentes algoritmos de criptografia e analisá-los comparativamente, a fim de auxiliar na garantia da confidencialidade, integridade e disponibilidade dos dados e minimizar potenciais ataques e invasões. Este estudo é relevante, pois aborda um tema atual e cada vez mais crescente dentro da realidade corporativa, a segurança dos dados.

1. Referencial Teórico

1.1 Segurança da Informação

Bastos e Caubit (2009, p. 17) definem o conceito de Segurança da Informação como:

> […] uma aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel.

Campos (2007) defende que a informação é composta de dados e componente do conhecimento, conforme ilustrado na Figura 1, e é o elemento

essencial para tomada de decisões e representa valor para o negócio. Além disso, a informação é um patrimônio da organização que deve ser protegida e preservada. De acordo com Claro (2013), os termos dado, informação e conhecimento podem ser entendidos como um elemento em sua forma bruta que sozinho não conduz a uma compreensão de determinado fato ou situação; um conjunto de dados coletados, organizados, ordenados, aos quais são atribuídos significado e contexto. As informações são utilizadas para trilhar novas possibilidades ou gerar inovações. Com base nestes conceitos, o conhecimento é o elemento principal para o sucesso de uma empresa, visto que gera valor para a organização.

Figura 1. Informação é a base do conhecimento
Fonte: Adaptado (CAMPOS, 2007)

O conceito de segurança da informação possui três atributos básicos, isto é, Integridade, Disponibilidade e Confidencialidade. A definição destes conceitos é consolidada na literatura (Tabela 1) (CAMPOS, 2007; MAURÍCIO ROCHA LYRA, 2008; DOUGLAS E. COMER, 2007; GURGEL et al., 2015).

Pode-se dizer que houve um incidente de segurança quando houver a quebra de pelo menos um desses princípios (CAMPOS, 2007).

Tabela 1. Atributos Básicos de Segurança da Informação

Integridade	Atributo que impede que a informação seja alterada e/ou danificada. Este atributo procura garantir que a informação não seja modificada sem a autorização explícita do proprietário. Entende-se “modificações”, qualquer alteração no conteúdo, remoção ou

	implantação de informações.
Confidencialidade	Garante que as informações só sejam acessadas pelo proprietário ou por pessoas autorizadas, atua no princípio de privacidade.
Disponibilidade	Atributo que garante a disponibilidade do acesso à informação. A informação deve estar acessível, para as entidades autorizadas, sempre que necessário.

Fonte: Adaptado (CAMPOS, 2007)

1.2 Criptografia de dados

Como forma de garantir a integridade e confidencialidade dos dados, sistemas de criptografia foram propostos por diversos pesquisadores (SOUSA, 2009). A criptografia de dados tem como objetivo codificar os dados que serão transmitidos, de modo que o conteúdo da mensagem não possa ser conhecido por terceiros. Os dados só podem ser decodificados pelo transmissor e receptor que possuem a chave criptografada. Essa chave é um código sigiloso que criptografa e descriptografa a mensagem por meio de um algoritmo. Segundo Sousa (2009), há dois tipos de criptografias (Tabela 2):

Tabela 2. Tipos de Criptografias

Criptografia de chave simétrica	Utiliza uma única chave para codificar e decodificar a mensagem, assim tanto o emissor quanto o receptor conhecem a chave utilizada. Portanto, manter a chave em sigilo é determinante para a confidencialidade dos dados.
Criptografia de chave assimétrica	Utiliza duas chaves distintas, sendo uma para codificar (chave pública), e uma para decodificar (chave privada). O que for criptografado com a chave pública só poderá ser descriptografado com a chave privada.

Fonte: Adaptado (SOUSA, 2009)

A criptografia de chave simétrica é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é rápido. Entretanto, esta é pouco escalável e necessita de um meio de comunicação seguro entre o transmissor e o receptor para o compartilhamento da chave (CERT.BR, 2012). Dentre os algoritmos de criptografia de chaves simétricas (Tabela 3), os mais comuns são o DES (do inglês, *Data Encryption Standard*), o IDEA (do inglês, *International Data Encryption Algorithm*) e o RC (do inglês, *Ron's Code ou Rivest Cipher*) (GURGEL et al., 2015).

Tabela 3. Algoritmos de criptografia de chaves simétricas

DES	Criado pela IBM em 1977, usa chaves de 56 bits e permite até 72 quatrilhões de combinações. Foi desvendado utilizando a técnica chamada de "força bruta" ou tentativa e erro.
IDEA	Criado em 1991 por James Massey e Xuejia Lai, usa chaves de 128 bits e tem estrutura semelhante ao DES, pois possui um número fixo de iterações de uma mesma função que utiliza subchaves distintas.
RC	Criado por Ron Rivest na empresa RSA Data Security, usa chaves de 8 a 1024 bits. RC2, RC4, RC5 e RC6 são versões do algoritmo RC, porém cada uma delas trabalha com chaves de maior complexidade.

Fonte: Adaptado (GURGEL et al., 2015)

A criptografia de chave assimétrica resolve o problema da necessidade de um meio seguro entre o transmissor e o receptor, pois utiliza-se duas chaves distintas, sendo uma para codificar (chave pública), e uma para decodificar (chave privada). Em vista disso, o transmissor não precisa se preocupar em transmitir a chave para o receptor para decodificar a mensagem. Porém, a criptografia de chave assimétrica é mais lenta em comparação à criptografia de chave simétrica (CERT.BR, 2012). Dentre os algoritmos de criptografia de chaves assimétricas (Tabela 4), os mais comuns são RSA (do inglês, *Rivest, Shamir and Adleman*) e o ElGamal (GURGEL et al., 2015).

Tabela 4. Algoritmos de criptografia de chaves assimétricas

RSA	Criado em 1977 no Massachusetts Institute of Technology (MIT), é um dos algoritmos de criptografia de chave assimétrica mais utilizados e o único algoritmo assimétrico que pode ser utilizado no Brasil, por entidades que emitem certificados digitais, as Autoridades Certificadoras (AC).
ElGamal	Criado por Taher ElGamal em 1984, algoritmo que obtém sua segurança utilizando de cálculos de logaritmos discretos.

Fonte: Adaptado (GURGEL et al., 2015)

1.3 Tipos de Ataques sobre mensagens encriptadas

Na literatura há diferentes tipos de ataques à criptografia, entretanto o criptoanalista deve possuir algum conhecimento do algoritmo de encriptação utilizado para conseguir decifrar um texto. Conforme Stallings (2015) os tipos de ataques à criptografia são:

Tabela 5. Tipos de ataques sobre mensagens encriptadas

Ataque de texto cifrado	O criptoanalista possui uma ampla quantidade de mensagens cifradas, mas desconhece as originais e as chaves utilizadas.
Ataque de texto conhecido	O criptoanalista possui uma ampla quantidade de mensagens cifradas e também as mensagens originais equivalentes.
Ataque adaptativo do texto escolhido	O criptoanalista tem à sua disposição um pequeno conjunto de dados e analisa os resultados.
Ataque do texto cifrado escolhido	O criptoanalista possui uma mensagem criptografada específica para ser decodificada.

Ataque de chave escolhida	O criptoanalista testa o sistema com chaves diferentes ou pode convencer os usuários do sistema a utilizarem determinadas chaves. Neste último caso, a finalidade é decifrar as mensagens criptografadas com essas chaves.

Fonte: Adaptado (STALLINGS, 2015)

1.4 Criptoanálise

A criptoanálise é uma ciência que desenvolve as técnicas capazes de "quebrar" as cifras, de modo a obter o texto original, mesmo que parcialmente, a partir do texto cifrado. Existem basicamente duas técnicas de criptoanálise (Tabela 6) (STALLINGS, 2015).

Tabela 6. Técnicas de criptoanálise

Ataques criptoanalíticos	Utiliza-se da natureza do algoritmo e eventualmente de algum conhecimento das características do algoritmo para tentar deduzir um texto claro (texto antes de ser encriptado).
Ataques por força bruta	O criptanalista testa todas as chaves possíveis em uma parte do texto cifrado, até conseguir uma tradução compreensível.

Fonte: Adaptado (STALLINGS, 2015)

2. Metodologia

Este trabalho compreende a realização de testes de criptoanálise, a fim de verificar a segurança dos algoritmos utilizados e efetuar um comparativo entre esses algoritmos. Para tanto, foram selecionados dois algoritmos, ambos de criptografias de chave simétrica, a Cifra de César, por ser um algoritmo simples e rápido de encriptação, e a Cifra de Vegenère, por ser uma cifra mais complexa de ser encriptada, portanto mais difícil de ser "quebrada" e requer que o criptoanalista tenha conhecimento da chave utilizada para encriptar.

A Cifra de César é uma técnica de encriptação por substituição clássica,

envolve substituir cada letra do alfabeto por uma letra localizada três posições adiante. A técnica de substituição visa substituir as letras do texto original por outras letras, números ou símbolos. No caso da Cifra de César é utilizado somente letras (STALLINGS, 2015).

A Cifra de Vigenère é uma técnica de criptografia por substituição polialfabética, onde cada letra é representada por um inteiro e utiliza uma chave para criptografar. Para cifrar soma-se os valores em inteiro que corresponde cada letra do texto a ser criptografado e os valores que correspondem à chave. Em seguida substitui os valores resultantes em texto cifrado (MARQUES, 2013).

Para testar ambos os algoritmos foi utilizada a frase “Security and Privacy in Applications”, por não possuir caracteres especiais, pois alguns algoritmos de criptografia não reconhecem o til, cedilha e crase, presentes na língua portuguesa. A frase foi retirada da revista científica IEEE Communications Magazine (ZHANG, 2017) e representa o texto a ser criptografado. A partir desta frase foi gerado o texto cifrado, por meio das cifras, isto é, algoritmos, selecionadas neste trabalho. Posteriormente, o texto original foi obtido a partir do texto cifrado, conforme apresentado na Seção 4.

3. Resultados

3.1 Cifra de César

Na Tabela 7 é apresentado o texto original, texto que será encriptado, e o texto cifrado utilizando o algoritmo de César.

Tabela 7. Texto claro e texto cifrado a partir do algoritmo de César

Texto Original:	security and privacy in applications
Texto Cifrado:	VHFXULWB DQG SULYDFB LQ DSSOLFDWLRQV

Fonte: Elaborado pelo autor.

Utilizando a técnica de criptoanálise por força bruta e experimentando as 25 chaves possíveis, equivalente ao número de organizações das letras existentes no alfabeto que podem ser obtidas na primeira coluna da Tabela 8, onde cada linha corresponde a uma possível chave (Tabela 8):

Tabela 8. Técnica de criptoanálise por força bruta

Chave	VHFXULWB	DQG	SULYDFB	LQ	DSSOLFDWLRQV
1	UGEWTKVA	CPF	RTKXCEA	KP	CRRNKECVKQPU
2	TFDVSJUZ	BOE	QSJWBDZ	JO	BQQMJDBJUPOT
3	SECURITY	AND	PRIVACY	IN	APPLICATIONS
4	RDBTQHSX	ZMC	OQHUZBX	HM	ZOOKHBZSHNMR
5	QCASPGRW	YLB	NPGTYAW	GL	YNNJGAYRGMLQ
6	PBZROFQV	XKA	MOFSXZV	FK	XMMIFZXQFLKP
7	AOYQNEPU	WJZ	LNERWYU	EJ	WLLHEYWPEKJO
8	NZXPMDOT	VIY	KMDQVXT	DI	VKKGDXVODJIN
9	MYWOLCNS	UHX	JLCPUWS	CH	UJJFCWUNCIHM
10	LXVNKBMR	TGW	IKBOTVR	BG	TIIEBVTMBHGL
11	KWUJMLQ	SFV	HJANSUQ	AF	SHHDAUSLAGFK
12	JVTLIZKP	REU	GIZMRTP	ZE	RGGCZTRKZFEJ
13	IUSKHYJO	QDT	FHYLQSO	YD	QFFBYSQJYEDI
14	HTRJGXIN	PCS	EGXKPRN	XC	PEEAXRPIXDCH
15	GSQIFWHM	OBR	DFWJOQM	WB	ODDZWQOHWCBG
16	FRPHEVGL	NAQ	CEVINPL	VA	NCCYVPNGVBAF
17	EQOGDUFK	MZP	BDUHMOK	UZ	MBBXUOMFUAZE
18	DPNFCTEJ	LYO	ACTGLNJ	TY	LAAWTNLETZYD
19	COMEBSDI	KXN	ZBSFKMI	SX	KZZVSMKDSYXC
20	BNLDARCH	JWM	YAREJLH	RW	JYYURLJCRXWB
21	AMKCZQBG	IVL	XZQDIKG	QV	IXXTQKIBQWVA
22	ZLJBYPAF	HUK	WYPCHJF	PU	HWWSPJHAPVUZ
23	YKIAXOZE	GTJ	VXOBGIE	OT	GVVROIGZOUTY
24	XJHZWNYD	FSI	UWNAFHD	NS	FUUQNHFYNTSX
25	WIGYVMXC	ERH	TVMZEGC	MR	ETTPMGEXMSRW

Fonte: Elaborado pelo autor

Após o emprego das 25 chaves foi possível obter o texto original (Chave 3). Uma vantagem de utilizar o algoritmo de César é a técnica de criptografia ser simples de ser realizada. Como desvantagens são a possibilidade de descobrir o texto original utilizando a criptoanálise por força bruta, pois existe apenas 25 chaves para experimentar, e a possibilidade de decodificar todo um texto cifrado descobrindo como parte dele é codificado. O algoritmo de César é bastante utilizado em uso didático e compõe parte de outros algoritmos de encriptação, como o algoritmo Rot13 que é uma variante do algoritmo de César (MANOJ, 2010).

3.1.1 Implementação em C

A Cifra de César foi implementada na linguagem C, conforme apresentado no Algoritmo 1.

Algoritmo 1. Implementação da Cifra de César em Linguagem C

```c
#include <stdio.h>
int main()
{
    char textoclaro[50], aux[50];
    int i;
    printf("\n Entre com o texto a sr criptografado: \n \n ");
    scanf(" %s", textoclaro);

        while(textoclaro[i] != '\0')
        {
            aux[i] = textoclaro[i] + 3;
            if((textoclaro[i] + 3) > 122)
            {
                aux[i] -=26;
            }
            if((textoclaro[i] + 3) < 97)
            {
                aux[i] += 26;
            }
            i++;
        }
        aux[i] = '\0';
        printf("\n \n Texto cifrado: %s \n \n \n ", aux);

        if(3%5 == 0)
        {
            printf("\n\n");
        }
    return 0;
}
```

Fonte: Elaborado pelo autor.

Primeiramente é solicitado que o usuário que entre com a palavra ou frase a ser criptografada. Em seguida, o texto cifrado é gerado utilizando o algoritmo de César. Verifica-se que a cifra gerada corresponde ao texto cifrado (Tabela 7), o que mostra o correto funcionamento do código.

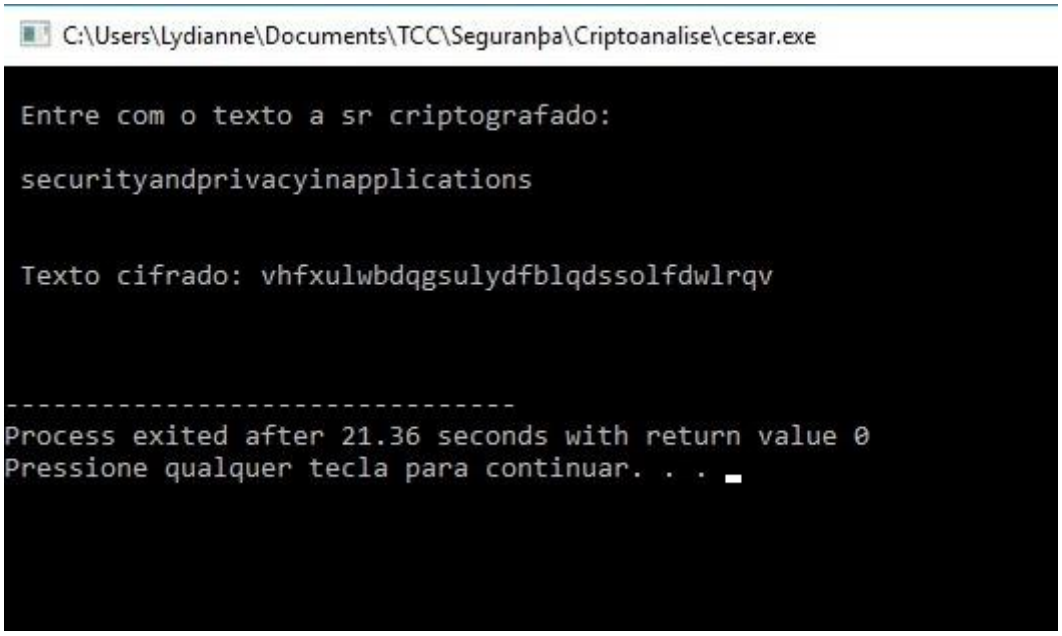


Figura 2. Código compilado do algoritmo de César
Fonte: Elaborado pelo autor.

3.2 Cifra de Vigenère

Nesta etapa, o texto original (Security and Privacy in Applications) foi transformado em números e a palavra-chave cripto foi utilizada. Para cada letra do alfabeto foi atribuído um número inteiro (Tabela 9).

Tabela 9. Correspondência entre números e letras

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	15	16	17	18	19	20	21	22	23	24	25		

Fonte: Elaborada pelo autor.

Para a cifra de Vigenère, primeiramente foi atribuído um valor (número

inteiro) a cada letra do texto a ser criptografado. Além disso, uma chave, que pode ser uma palavra ou uma frase, foi utilizada para a criptografia. Neste trabalho, a palavra “cripto” foi utilizada como chave. Os valores em inteiro do texto a ser criptografado foram somados aos valores da chave escolhida e o resultado, em inteiros, foi substituído pelas letras correspondentes, conforme a (Tabela 10). Na primeira coluna está o texto a ser criptografado. Na segunda coluna está o valor em inteiro do texto. A terceira coluna corresponde a chave utilizada. É importante notar que a palavra-chave se repete. Na quarta coluna encontra-se o valor em números correspondente à chave. Na quinta coluna é apresentada a soma dos valores do texto a ser cifrado e da chave. Na sexta coluna quando a soma dos valores é maior que 26, é subtraído 26 (número de letras do alfabeto). Por fim, na sétima coluna, o texto criptografado.

Tabela 10. Técnica de encriptação do algoritmo de Vigenère

Texto original	Valor do texto	Chave	Valor da chave	Soma dos valores	Resultado da soma (26)	Texto criptografado
S	18	C	2	20	20	U
E	4	R	17	21	21	V
C	2	I	8	10	10	K
U	20	P	15	35	9	J
R	17	T	19	36	10	K
I	8	O	14	22	22	W
T	19	C	2	21	21	V
Y	24	R	17	41	15	P
A	0	I	8	8	8	I
N	13	P	15	28	2	C
D	3	T	19	22	22	W
P	15	O	14	29	3	D
R	17	C	2	19	19	T
I	8	R	17	5	5	F
V	21	I	8	29	3	D
A	0	P	15	15	15	P
C	2	T	19	21	21	V

Y	24	O	14	38	12	M
I	8	C	2	10	10	K
N	13	R	17	30	4	E
A	0	I	8	8	8	I
P	15	P	15	30	4	E
P	15	T	19	34	8	I
L	11	O	14	25	25	Z
I	8	C	2	10	10	K
C	2	R	17	19	19	T
A	0	I	8	8	8	I
T	19	P	15	34	8	I
I	8	T	19	27	1	B
O	14	O	14	28	2	C
N	13	C	2	15	15	P
S	18	R	17	35	9	J

Fonte: Elaborada pelo autor.

O texto cifrado gerado a partir da frase selecionada é UVKJKWVP ICW DTFDPVM KE IEIZKTIIBCPJ. Na Tabela 11 é apresentado o texto original, que será encriptado, e o texto cifrado, utilizando a técnica de encriptação do algoritmo de Vigenère.

Tabela 11. Texto original e texto cifrado a partir do algoritmo de Vigenère

Texto Original:	security and privacy in applications
Texto Cifrado:	UVKJKWVP ICW DTFDPVM KE IEIZKTIIBCPJ

Fonte: Elaborado pelo autor

Para descriptografar o texto cifrado pelo algoritmo de Vigenère é necessário que o criptoanalista tenha conhecimento da palavra-chave utilizada para encriptar, ou seja, a palavra cripto, e fazer uso do quadrado de Viginère, tabela criada por Blaise de Vigenère para a realização prática deste algoritmo contendo todos os alfabetos possíveis de serem utilizados (Tabela 12).

Tabela 12. Quadrado de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Fincatti (2010)

Para a decodificação do texto criptografado, primeiramente é necessário ter conhecimento da chave cripto e do texto codificado, UVKJKWVP ICW DTFDPVM KE IEIZKTIIBCPJ. Posteriormente, os seguintes passos foram realizados. No passo 1, a coluna da primeira letra da palavra cripto (o “C”) foi selecionada e percorrida até a letra “U” (primeira letra criptografada). A linha referente à letra U corresponde a primeira letra do texto original, a letra “S”, conforme indicado na Tabela 13.

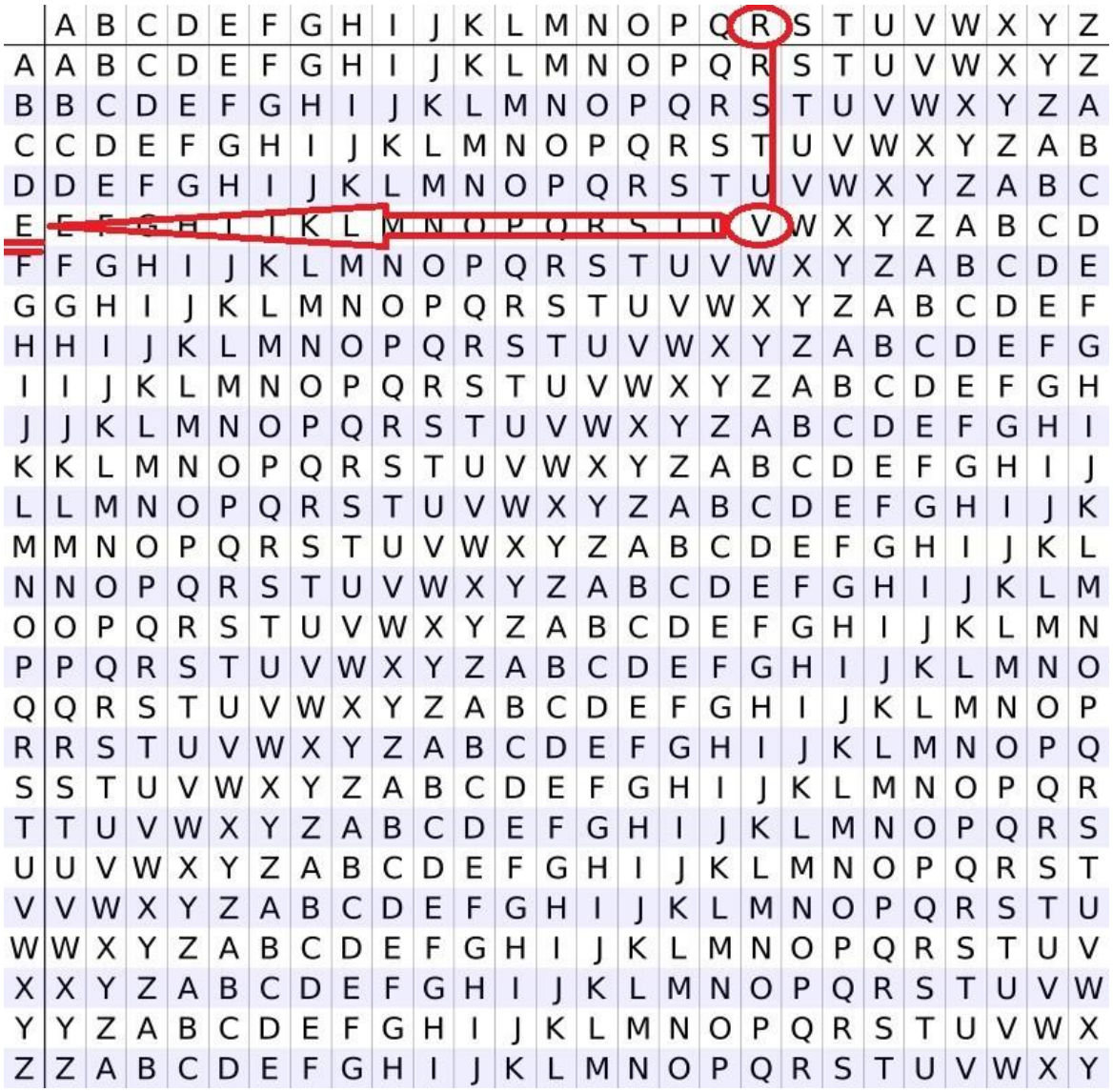
Tabela 13. Quadrado de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Adaptado (FINCATTI, 2010)

No passo 2, a coluna da letra “R” (segunda letra da palavra cripto) foi selecionada e percorrida até visualizar a letra “V” (segunda letra criptografada). A linha referente à letra V corresponde a segunda letra do texto original, a letra “E”, conforme indicado na Tabela 14.

Tabela 14. Quadrado de Vigenère.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Adaptado (FINCATTI, 2010)

Em seguida foi realizado o mesmo procedimento para as letras seguintes até que toda a frase foi descriptografada, sendo possível obter o texto original “Security and Privacy in Applications”. As vantagens em utilizar o algoritmo de Vigenère são que a técnica de criptografia do algoritmo de Vigenère possui maior complexidade comparado ao algoritmo de César e o criptoanalista necessita conhecer a palavra-chave utilizada na encriptação para obter o texto descriptografado. Por outro lado, as desvantagens em utilizar o algoritmo de Vigenère é manter a confidencialidade da chave e a possibilidade de se decodificar todo um texto cifrado descobrindo como parte dele é codificado.

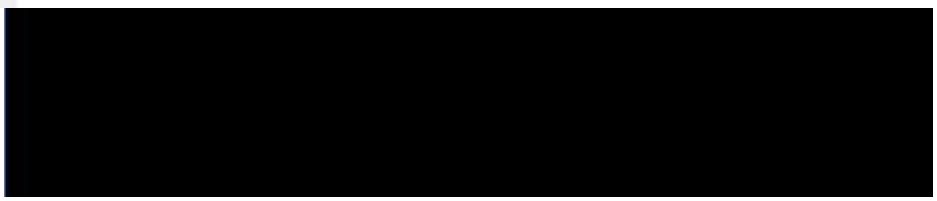
3.2.1 Implementação em C

A Cifra de Vigenére foi implementada em linguagem, conforme o Algoritmo 2.

Algoritmo 2. Implementação da Cifra de Vigenère em Linguagem C

Primeiramente é solicitado ao usuário que entre com o texto a tografado. Em seguida, solicita que o usuário digite a chave que s zada para criptografar. Por meio do algoritmo de Vigenère é gerado o te ado e, posteriormente, verifica-se se a cifra gerada corresponde ao te ado na Tabela 11.

```c
#include <stdio.h>

int main()
{
    char textoclaro[50], textocifrado[50], chave[20];
    int i=0, tam=0;

    printf("\n \n Entre com o texto a ser criptografado: ");
    scanf("%s", &textoclaro);

    printf("\n \n Entre com a chave: ");
    scanf("%s", &chave);

        while(chave[tam]!=0)tam++;

            while(textoclaro[i]!=0) {

                textocifrado[i] = (((textoclaro[i]-97)+(chave[i%tam]-97))%26)+97; i++;
            }

        textocifrado[i]=0;

        printf(" \n \n Texto Cifrado: %s\n \n \n", textocifrado);

    system("PAUSE");

    return 0;
}
```



Fonte: Elaborado pelo autor.

3.3 Comparativo entre as cifras utilizadas

Informações	Cifra de César	Cifra de Vigenère
Classe	Substituição simples	Substituição utilizando palavra-chave
Tipo	Monoalfabética, pois usa apenas um alfabeto cifrante e trata cada um dos caracteres individualmente	Polialfabética, pois utiliza vários alfabetos cifrantes
Nível de segurança	Baixa	Média, pois necessita do conhecimento da palavra-chave para descriptografar
Uso	Pode ser utilizada em textos longos e curtos	Pode ser utilizada em textos longos e curtos
Criptoanálise	Uma criptoanálise baseada na característica da língua é suficiente para descriptografar um texto.	Necessita de algum conhecimento do algoritmo de criptografia, como a chave utilizada.

Considerações finais

Neste trabalho foi exposto a importância da segurança da informação em um ambiente empresarial e que o avanço da tecnologia traz consigo numerosos benefícios. Contudo, a proliferação de novas tecnologias e de mais pessoas se envolvendo com a arte da programação faz crescer os desafios para combater as novas ameaças e ataques que surgem. Neste contexto, a criptografia de dados é importante para a proteção de mensagens, para que as interceptações externas não acarretem no vazamento de informações sigilosas.

Ainda, este trabalho teve como objetivo utilizar a criptoanálise para testar os algoritmos Cifra de César e Cifra de Vigenère e analisá-los comparativamente, a fim de auxiliar na garantia da Confidencialidade, Integridade e Disponibilidade dos dados e minimizar potenciais ataques. Tratou-se de uma pesquisa a qual apontou os tipos de ataques sobre mensagens

encriptadas, o conceito de criptografia de dados e como a criptoanálise pode ajudar na escolha de algoritmos mais eficientes. Além disso, apresentou os resultados das técnicas capazes de “quebrar” as cifras utilizadas, de modo a obter o texto original. Por fim, foi realizado um comparativo entre as cifras utilizadas e efetuada a implementação em linguagem C dos algoritmos de encriptação selecionados.

Referências

BASTOS, A.; CAUBIT, R. **Gestão de Segurança da Informação:** uma visão prática ISO 27001 e 27002. Rio de Janeiro: [s.n.], 2009.

CAMPOS, A. **Sistema de Segurança da Informação**. 2. ed. Florianópolis: [s.n.], 2007.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet.** 2012. Disponível em: <https://cartilha.cert.br/seguranca/>. Acesso em: 7 nov. 2018.

CLARO, A. **Sistemas de Informações Gerenciais**. São Paulo: [s.n.], 2013.

COMER, D. E. **Redes de computadores e internet**. 4. ed. Porto Alegre: [s.n.], 2007.

FINCATTI, C. A. **Criptografia como agente motivador na aprendizagem da matemática em sala de aula**. São Paulo: [s.n.], 2010.

GURGEL, P. H. M. et al. **Redes de Computadores:** da teoria à prática com Netkit. Elsevier brasil. [S.l.: s.n.], 2015.

LYRA, M. R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

_____. **Governança da Segurança da Informação**. Brasília, DF: [s.n.], 2015.

MANOJ, I. Venkata Sai. Cryptography and steganography. **International Journal of Computer Applications (0975 – 8887),** v. 1, n. 12, 2010.

MARQUES, T. V. **Criptografia:** abordagem histórica, protocolo Diffie-Hellman e aplicações em sala de aula. 2013. 76 f. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal da Paraíba, 2013.

SOUSA, L. B. D. **Redes de Computadores:** guia total. São Paulo: [s.n.], 2009.

STALLINGS, W. **Criptografia e Segurança de Redes**. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

XAVIER, R.; MENDES, L.; MONTEIRO, A. **Assinatura digital:** utilização na segurança de software. 2. ed. Santos Dumont: [s.n.], 2015.

ZANG, K. et al. Security and Privacy in Smart City Applications: Challenges and Solutions. **IEEE Communications Magazine,** v. 55, issue 1, p. 122-129, jan. 2017.