Técnica criptográfica simétrica utilizando algoritmo XOR

Lucas Emmanuel
RU 3635989
Disciplina: Matemática Computacional
Curso: Análise e Desenvolvimento de Sistemas

Resumo

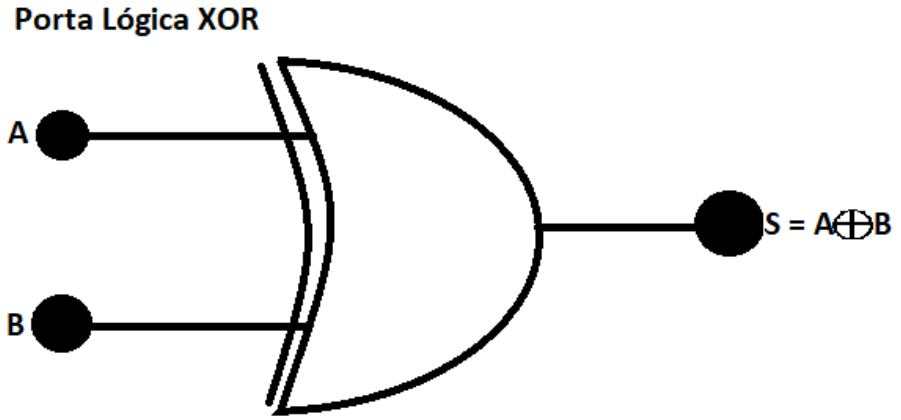
Nesta atividade será demonstrado o uso da técnica criptográfica simétrica com o algoritmo elementar XOR, utilizando o RU como base para chave criptográfica. Codificando e decodificando as oito primeiras letras do nome do aluno comprovando a reciprocidade do processo.

Introdução

A criptografia é um ramo matemático que trata do processo de transformação da informação do seu estado original ***texto claro*** para um formato protegido ***texto cifrado*** com a ocultação de seu significado. Tem como principal objetivo manter a integridade, segurança e confidencialidade da informação.

Resumo da técnica

XOR é uma operação comum aos processadores. Trata-se de uma operação binária com função de detectar desigualdades, fornecendo valores de saída quando duas entradas são diferentes. Consiste de uma operação bastante simples e performática, amplamente utilizada nos processos criptográficos.



A	B	S = A⊕B
0	0	0
0	1	1
1	0	1
1	1	0

Para realizar a criptografia com o uso do XOR, transforma-se o texto claro em binário com uso da tabela ASCII. Utiliza-se uma chave criptográfica também convertida diretamente em binário, e logo depois efetua-se a operação XOR bit a bit. Neste exemplo, estarei efetuando múltiplas somas entre os algarismos que compõem o RU N° **3635989** (**3+6+3+5+9+8+9**) e utilizando o valor resultante convertido em binário como chave criptográfica. Valor resultante da soma: **43**.

Desenvolvimento

Para efetuar a conversão do dígito 43 efetua-se sucessivas divisões por dois até que o quociente seja igual a zero. Logo após é obtido o valor convertido em binário, como no exemplo abaixo:

$$43/2 = 21, \text{ resto} = 1$$
$$21/2 = 10, \text{ resto} = 1$$
$$10/2 = 5, \text{ resto} = 0$$
$$5/2 = 2, \text{ resto} = 1$$
$$2/2 = 1, \text{ resto} = 0$$
$$1/2 = 0, \text{ resto} = 1$$
$$(43)_{10} = (101011)_2$$

Logo a nossa chave binária é **00101011**. Agora aplicamos o algoritmo XOR bit a bit para obter a cifra (código em binário codificado) como no exemplo a seguir :

EXEMPLO:

Caracter **"C"** em ASCII: 67 ou **0100 0011**
Chave Criptográfica: **"A"** em ASCII: 65 ou **0100 0001**

Aplicando operação XOR:

0100 0011
0100 0001

CIFRA A ⊕ B: 0000 0010

Em seguida iremos aplicar a mesma técnica demonstrada acima para codificar os ***oito primeiros caracteres*** do nome do aluno da vigente atividade, neste caso **Lucas Emmanuel**.

Primeiramente, converteremos todos os caracteres em seus correspondentes binários:

CARACTER	ASCII	BINÁRIO	Nº
L	76	0100 1100	1
u	117	0111 0101	2
c	99	0110 0011	3
a	97	0110 0001	4
s	115	0111 0011	5
Espaço	32	0010 0000	6
E	69	0100 0101	7
m	109	0110 1101	8

Feito isso, iremos aplicar a técnica XOR nos correspondentes binários para gerar uma cifra codificada, e logo em seguida converteremos a mesma em caracteres:

CARACTER	L	u	c	a	s	Espaço	E	m
BINÁRIO	0100 1100	0111 0101	0110 0011	0110 0001	0111 0011	0010 0000	0100 0101	0110 1101
CHAVE BINÁRIA	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011
CIFRA	0110 0111	0101 1110	0100 1000	0100 1010	0101 1000	0000 1011	0110 1110	0100 0110
CODIFICADO	g	^	H	J	X	VT	n	F

LEGENDA

VT = Tabulação Vertical
(Caracter de controle)

Ao término do processo temos a seguinte informação codificada: **g^HJXVTnF**

Para descodificar a informação, aplicamos novamente a técnica de forma inversa:

a) Converter os caracteres codificados em seus respectivos correspondentes binários
b) Aplicar a técnica do algoritmo elementar XOR
c) Obter a informação decodificada

Como podemos visualizar na imagem a seguir:

CODIFICADO	g	^	H	J	X	VT	n	F
BINÁRIO	0110 0111	0101 1110	0100 1000	0100 1010	0101 1000	0000 1011	0110 1110	0100 0110
CHAVE BINÁRIA	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011	0010 1011
APLICAR XOR	0100 1100	0111 0101	0110 0011	0110 0001	0111 0011	0010 0000	0100 0101	0110 1101
DECODIFICADO	L	u	c	a	s	Espaço	E	m

Conclusão

Como visto acima, podemos utilizar a porta lógica XOR como ferramenta de codificação e decodificação de informações computacionais, pois a mesma oferece a possibilidade de efetuar operações lógicas de forma concisa, eficiente e com baixo custo de processamento, permitindo assim processar um grande número de informações em pouco tempo e com grande confiabilidade.

Esse tipo de criptografia mostra-se segura, pois para decifrá-la é necessário saber a chave utilizada e o processo criptográfico utilizado. Graças a criptografia é possível trocar informações entre duas ou mais partes, sem que haja perda, interceptação ou acesso indevido das mesmas, sem a autorização necessária. Pode ser utilizada em quaisquer atividades computacionais, como por exemplo em softwares que possuem dados que não podem ser alterados ou acessados, comprometendo assim o funcionamento e confidencialidade do mesmo.

Referências

Tabela ASCII *https://www.ime.usp.br/~kellyrb/mac2166_2015/tabela_ascii.html*

Imagens *Imagens produzidas pelo software microsoft paint com referências ao conteúdo ministrado nas aulas de matemática computacional da universidade UNINTER*