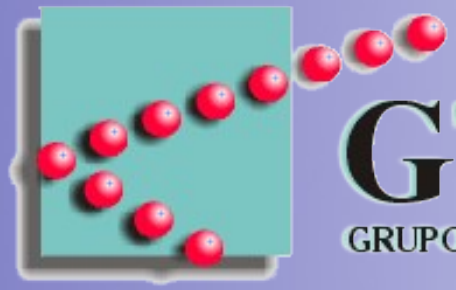

GTA / UFRJ

GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

REDES DE COMPUTADORES 1

CRIPTOGRAFIA QUÂNTICA

Alunos: Fábio Dias Lopez (ECA-108037654)

Luiz Antonio Viana Carapeto (ECA-108037696)

Victor Frangipani de Oliveira Lima (ECA-108037777)

Universidade Federal do Rio de Janeiro

Escola Politécnica

Índice

Universidade Federal do Rio de Janeiro
Escola Politécnica

1.Introdução à Criptografia

Tenta tornar secreta uma mensagem

Proteção de dados

Assinatura Digital

Utiliza métodos distintos de embaralhamento

Segurança X Preservação da mensagem

Universidade Federal do Rio de Janeiro
Escola Politécnica

Hieróglifos fora de ordem (1900 a.c.)

Cifra de Atbash

Cifra de César

Cifras de Substituição

Cifra de Vigenère

Criptografia aplicada com computação

Criptografia Simétrica:

DES (Data Encryption Standart)

AES (Advanced Encryption Standart)

Criptografia Assimétrica

Algoritmo RSA

Criptografia segura por modelos matemáticos

Tamanho da chave simétrica	chave possíveis	Tempo para quebrar
40	1 x 10^12 (1 trilhão)	2 horas
56	7 x 10^16	20 horas
64	2 x 10^19	9 anos
128	3 x 10^33	10^19 anos
256	1 x 10^77	10^58 anos

O Problema do Logaritmo Discreto

Maior capacidade de processamento: o qubit

Algoritmo de Schor

Comprimento do número a ser fatorado (em bits)	Tempo de fatoração por algoritmo clássico	Tempo de fatoração com o algoritmo de Shor
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quatrilhões de anos	4,8 horas

Universidade Federal do Rio de Janeiro
Escola Politécnica

3. Criptografia Quântica

Mecânica quântica aplicada a criptografia

Permite a detecção de intrusos

Criação de chaves

Segurança perfeita (com cifra de Verman)

Princípio da Incerteza de Heisenberg

Medição implica modificação

A Lei de Malus

Universidade Federal do Rio de Janeiro
Escola Politécnica

3. Criptografia Quântica

Protocolo BB84

Polarização e Base

Obtenção de chaves

Utiliza um canal público

Sequência aleatória de fótons										
Filtros usados por Bob	X	+	+	X	X	+	X	X	X	+
Resultados obtidos por Bob										
Sequência final secreta	0	0		1		0	1	0		

4. Vantagens e desvantagens

Maior segurança

Difícil implementação

Custo elevado

Taxa de erro muito alta

Distância limitada

5. Conclusão

A segurança é a base da criptografia quântica

A velocidade é a base da computação quântica

Os custos e a dificuldade de implementação freiam seu crescimento

Os atuais modelos ainda são confiáveis

Tendência de forte crescimento

Universidade Federal do Rio de Janeiro
Escola Politécnica

6. Perguntas

1) Por que é, ou será em um futuro próximo, necessário o uso de criptografia quântica para garantir a segurança de transmissões?

2) Que fundamento da mecânica quântica torna interessante o seu uso na criptografia?

3) Qual a principal aplicação da criptografia quântica hoje em dia?

4) Cite um dos problemas que impedem a adoção em larga escala da criptografia quântica com a tecnologia atual.

5) Qual a diferença entre computação e criptografia quântica?

7. Bibliografia

Livros:
BUCHMANN, J.A. Introduction to cryptography
SATOY, M. The Music of the Primes: Searching to Solve the Greatest Mystery in Mathematics
MAO, W. Modern Cryptography: Theory and Practice
MENEZES, A.J.; OORSCHOT, P.C.; VANSTONE, S.A. Handbook of applied cryptography (1996)
HENDRYCH, M. Experimental Quantum Cryptography
ANOOP, M. S., “Public Key Criptography”

Links:
http://tph.tuwien.ac.at/~oemer/doc/quprog/node18.html
http://www.inovacaotecnologica.com.br/index.php
http://tombuntu.com/index.php/2007/12/12/simple-file-encryption-with-openssl/
http://www.devco.net/archives/2006/02/13/public_-_private_key_encryption_using_openssl.php
http://www.gta.ufrj.br/grad/08_1/quantica/index.html
http://pt.wikipedia.org/wiki/Criptografia_quântica