ICMC USP
SÃO CARLOS

GANESH

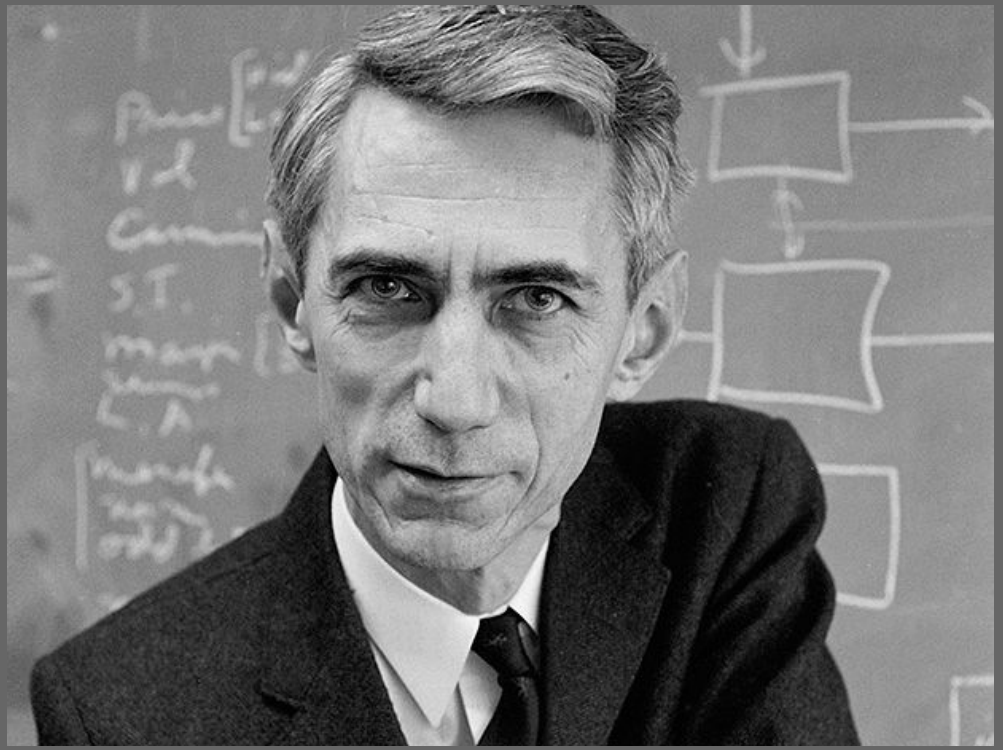
CRIPTOGRAFIA

O pai da criptografia moderna

Claude Shannon

Desenvolveu a Teoria da Informação, em particular o teorema da capacidade do canal

Criou diversos códigos

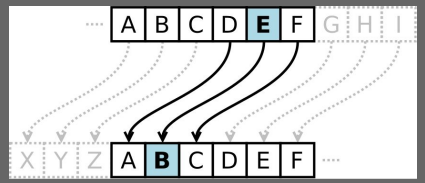


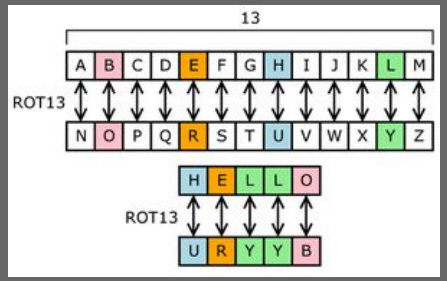
Conceitos Básicos

- Mensagem
- Código
- Cifra
  - Bloco
  - Fluxo

Operações Básicas

- Transposição
- Substituição
- OU-EXCLUSIVO
  - Verifica paridade

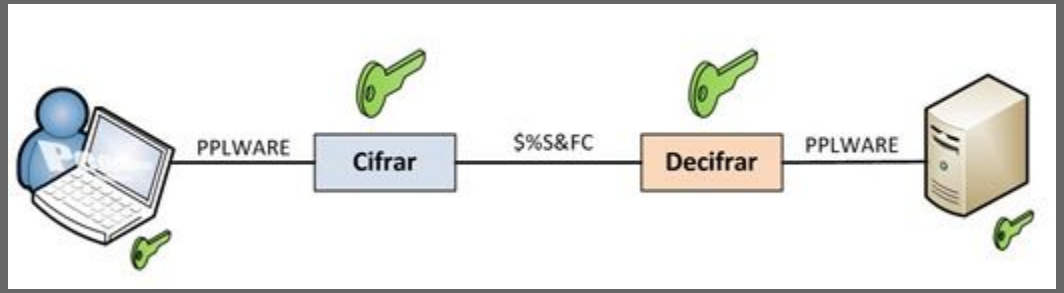




A	B	Saída
0	0	0
0	1	1
1	0	1
1	1	0

Criptografia Simétrica

- Usa a mesma chave para criptografar e descriptografar dados
- Tem como princípio a confidencialidade da chave

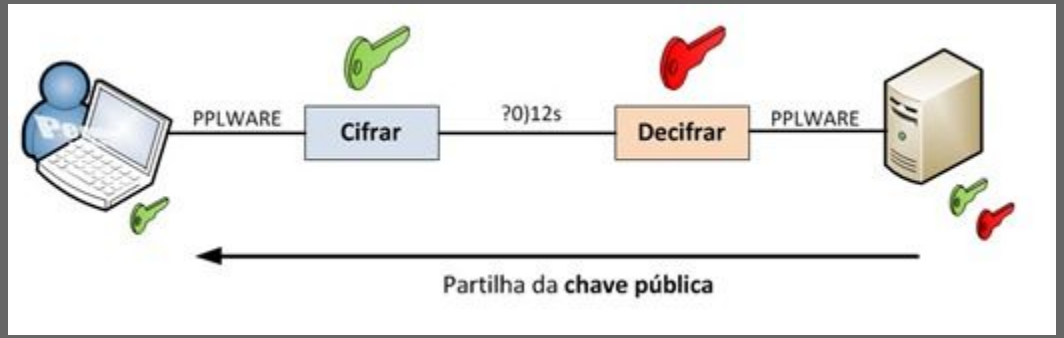


Criptografia Simétrica

- Stream Cipher
- Block Cipher
- Transmissão de chave precisa de uma canal seguro
- Série de ataques conhecidos que forçaram a geração de cifras com chaves grandes e processos longos

Criptografia Assimétrica

- Usa duas chaves diferentes
- Uma chave pública para criptografar, e uma chave privada para descriptografar dados
- Tem como princípios, além de confidencialidade, a integridade, autenticidade e não-repúdio



Criptografia Assimétrica

- Função alçapão
- Uma chave pode ser gerada a partir da outra
- Ataques de força bruta, chaves grandes protegem

Assinatura Digital

- Permite comprovar a autenticidade e a integridade de uma informação
- Baseia-se no fato de que apenas o dono conhece a chave privada
- A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

Bases numéricas

- Base Binária
- Base Octal
- Base Decimal
- Base Hexadecimal
- Base 32
- Base 64

Z2FuZXNoIGVoIGZlcmE=

Algoritmos Clássicos

- Cifra de César
- Atbash
- Rot13
- Cifra Afim
- Playfair
- Cifra de Vigenere
- Enigma
- One-time Pad

Algoritmos Modernos

- DES - Data Encryption Standard
- TRIPLE DES - Triple Data Encryption Standard
- AES - Advanced Encryption Standard
- Blowfish - Sucessor do AES
- Twofish - Sucessor do Blowfish
- RSA - Ron Rivest, Adi Shamir, Leonard Adleman
- Curvas Elípticas - Complexa, menor chave
- MD5 - Para hashes
- RC4 - Provado como inseguro

Exemplo com OpenSSL

Cria par de chaves pública e privada:

```
openssl genrsa -aes256 -out private.pem 2048
```

Separa a chave pública no arquivo public.pem:

```
openssl rsa -in private.pem -outform PEM -pubout -out public.pem
```

Links úteis

- https://pt.khanacademy.org/computing/computer-science/cryptography
- https://www.youtube.com/watch?v=YEBfamv-_do
- https://www.openssl.org/
- https://www.dcode.fr/v
- https://gchq.github.io/CyberChef/

Referências extras

- https://en.wikipedia.org/wiki/Cryptography
- https://en.wikipedia.org/wiki/Public-key_cryptography
- https://en.wikipedia.org/wiki/Symmetric-key_algorithm

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br