Introdução a Criptografia

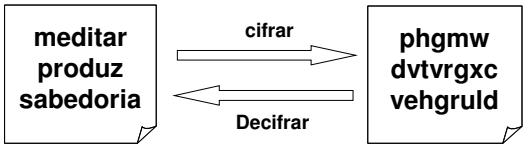
- **Necessidades**
  - Exigências por confidencialidade e privacidade
  - Originalidade ao documento eletrônico
  - Internet segura e confiável
- **Alternativa**

" arte ou a ciência de se escrever em cifras "

Criptografia (*kriptos* = oculto + *grifo* = grafia)

Introdução a Criptografia

- **Processos**



(texto plano) (texto cifrado)

Introdução a Criptografia

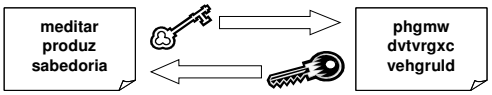
- **Algoritmos Criptográficos (cifradores)**
  - Quanto a segurança podem ser baseados:
    - segredo do algoritmo, *restritos*
    - segredo da chave, *kerchoff*

$Y = E_k(X) \iff X = D_k(Y)$

Introdução a Criptografia

- **Sistemas Criptográficos Simétricos**

- **Sistemas Criptográficos Assimétricos**



Introdução a Criptografia

- **Benefícios da Criptografia**
  - Confidencialidade, ou sigilo

" garantia de que, somente envolvidos no processo tem acesso a informação "

Introdução a Criptografia

- **Benefícios da Criptografia**
  - Confidencialidade, ou sigilo
  - Autenticidade, autoria

" garantia de identificação das entidades envolvidas no processo "

Introdução a Criptografia

- **Benefícios da Criptografia**
  - Confidencialidade, ou sigilo
  - Autenticidade, autoria
  - Não-repúdio, não-recusa

" garantia de que a entidade envolvida não irá negar no futuro sua ação "

Introdução a Criptografia

- **Outras Tecnologias**
  - HASH, função resumo

" garantia de que a informação não foi alterada ao longo de sua existência "

Introdução a Criptografia

- **HASH + Criptografia**
  - Assinatura Digital, Hash Cifrado

" garantia de integridade, autoria e não-repúdio "

Introdução a Criptografia

- **Tecnologia Paralela**
  - Criptoanálise

" abrange princípios, métodos e meios para descriptação de um criptograma, sem prévio conhecimento dos códigos e cifras usados na geração do texto cifrado "

Introdução a Criptografia

- **Segurança incondicional**
  - Imposível de ser quebrada
- **Segurança computacional**
  - Inviável de ser quebrada

Tamanho da chave (bits)	Possíveis chaves	Tempo requerido (1 cripto/μs)	Tempo (10^6 cripto/μs)
32	$2^{32} = 4.3\times10^{9}$	2^{31} μs = 35.8 min	2.15 ms
56	$2^{56} = 7.2\times10^{16}$	2^{55} μs = 1142 anos	10.01 hs
128	$2^{128} = 3.4\times10^{38}$	2^{127} μs=5.4×10^{24} anos	5.4×10^{18} anos