

Introdução a Criptografia

- **Necessidades**

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

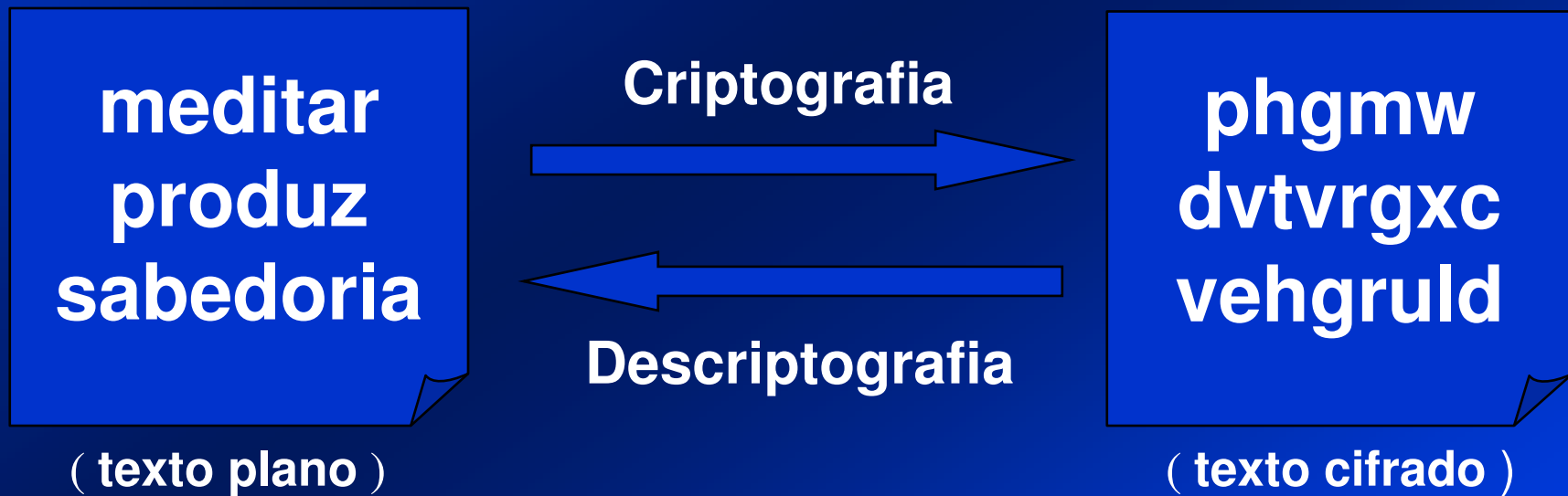
- **Alternativa**

“ arte ou a ciência de se escrever em cifras ”

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

Introdução a Criptografia

- Processos



Introdução a Criptografia

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

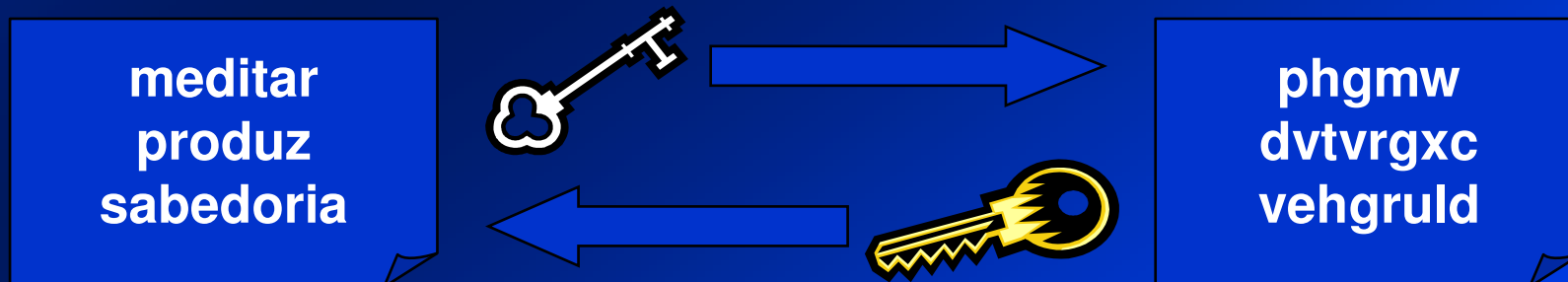
$$Y = E_k(X) \quad \longleftrightarrow \quad X = D_k(Y)$$

Introdução a Criptografia

- **Sistemas Criptográficos Simétricos**

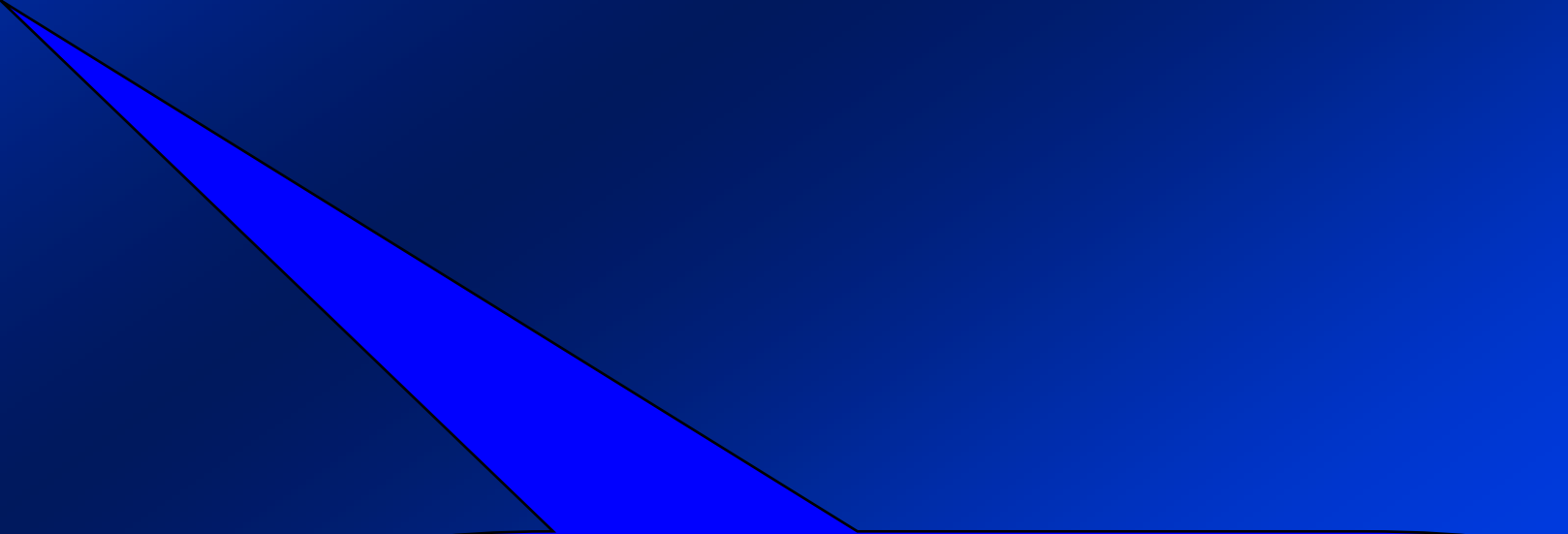


- **Sistemas Criptográficos Assimétricos**



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**

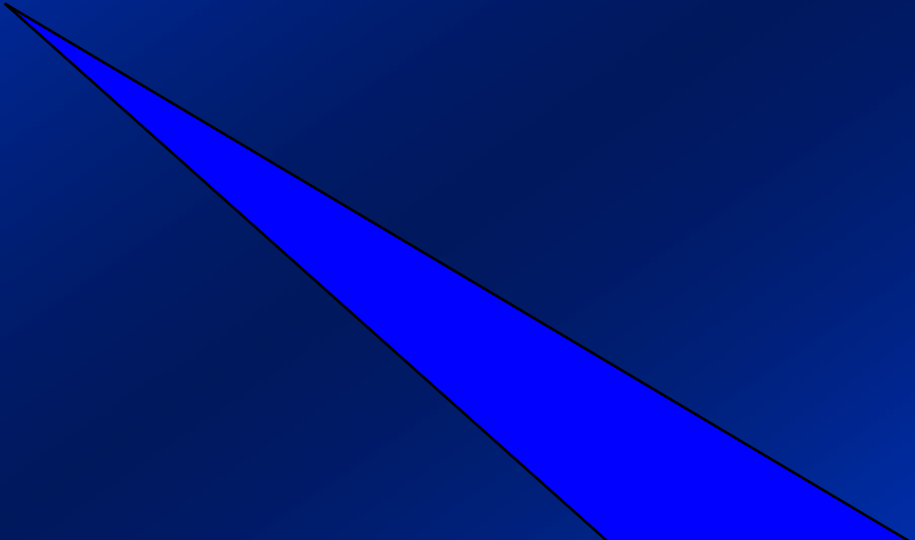
- **Confidencialidade, ou sigilo**
- **Autenticidade, autoria**
- **Não-repúdio, não-recusa**



“ 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 descrição de um criptograma, sem prévio conhecimento dos códigos e cifras usados na geração do texto cifrado “

Introdução a Criptografia

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

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