Criptografia

MICEI/MSDPA

José Carlos Bacelar Almeida
(jba@di.uminho.pt)

Informação sobre a disciplina

- Página da disciplina: http://lmf.di.uminho.pt/cripto-micei
- Atendimento: 6ª à tarde
- Avaliação:
  - Teste teórico (50%)
  - Pequenos projectos/apresentações (50%)

Objectivos da disciplina

Estudo dos fundamentos teóricos e de técnicas básicas da criptografia moderna.

Aplicações criptográficas correntes.

Segurança em protocolos criptográficos.

Programa resumido

- Fundamentos
- Técnicas criptográficas modernas
- Aplicações da criptografia
- Segurança em protocolos criptográficos

  - Palestras
  - Demos
  - Projectos

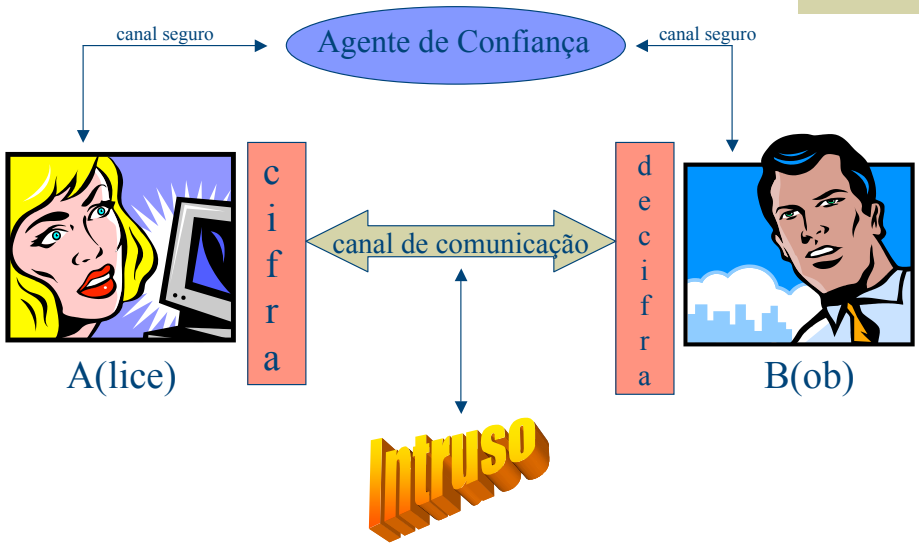
Criptografia (Kryptos+Graphein)

- Ciência (ou arte) de transmitir segredos.

  i.e., dispor da capacidade de comunicar uma mensagem de forma a que alguém, mesmo dispondo do controlo do canal de comunicação, não esteja habilitado a compreender o seu conteúdo.

- **Cripto-análise**: ciência (ou arte) de comprometer ("quebrar") sistemas criptográficos.

Modelo



Hipóteses para o intruso...

- Ataques ***passivos***

  Atribui-se ao intruso unicamente a capacidade de *escutar* o canal de comunicação (i.e. de observar todo o tráfego que circula no canal).

- Ataques ***activos***

  Atribui-se adicionalmente a capacidade para manipular a informação que circula no canal de comunicação (alterar/bloquear/injectar mensagens).

Propriedades de segurança

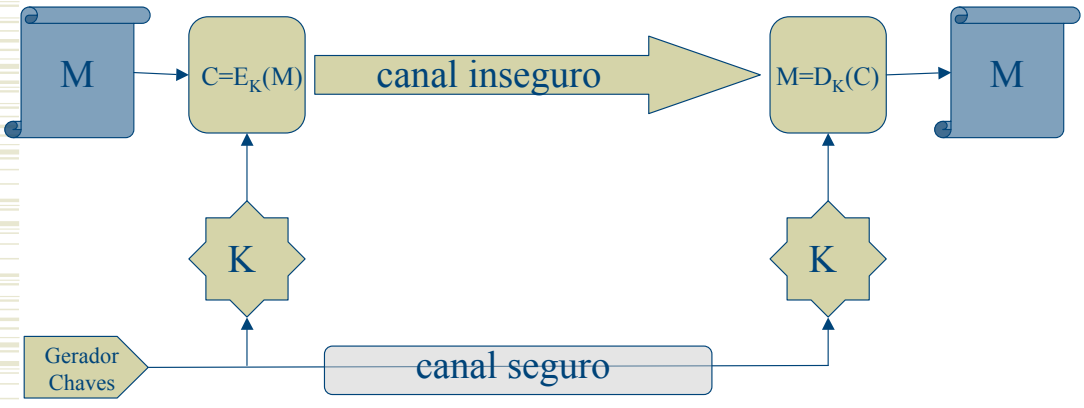
- Confidencialidade – garantir que o conteúdo da mensagem não é revelado.
- Integridade – garantir que o conteúdo da mensagem é preservado.
- Autenticidade – garantir que a origem da mensagem.
- Não repúdio – garantir que a produção da mensagem não pode ser negada.
- Entidade (identificação) – garantir a identificação de um agente perante outro.
- ...

Alguma terminologia

- **Texto limpo** – mensagem a transmitir.
- **Cifra** – operação que transforma o texto limpo numa mensagem sem conteúdo informativo: o **criptograma**
- **Chave** – parâmetro de segurança da operação de cifra.
- **Sistema criptográfico** – especificação das operações de cifra/decifragem.
- **Ataque** – comprometimento dos objectivos da técnica utilizada (e.g. obtenção do texto limpo sem conhecimento prévio da chave; obtenção da chave; etc.)

Sistema criptográfico clássico

$D_K(E_K(M)) = M$



Uma cifra da antiguidade

- Cifra de césar (Utilizada por Júlio César na campanha da Gália)
- Operação de cifra consiste num deslocamento pré-determinado do alfabeto

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z
+6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	W	Y	Z	A	B	C	D	E	F

- Exemplo: “IGWZGMUKYZGTUVGVU”

(CartagoEstaNoPapo)

- Nº de chaves: 26 (uma delas “**fraca**”)

Princípio de Kerckhoff

Para avaliar a segurança de uma técnica criptográfica devemos assumir que esta é do conhecimento de eventuais inimigos.

Corolário: toda a segurança resulta da chave utilizada.

Classificação de ataques

- Força bruta – é testado todo o espaço de chaves com vista a identificar a que decifra com sucesso o criptograma (pressupõe redundância na mensagem que permite identificar o "sucesso" da decifragem).
- Conhecimento do criptograma (só) – só se dispõe do conhecimento do(s) criptograma(s).
- Texto limpo conhecido – dispõe-se de um (ou vários) par(es) texto limpo/criptograma. O objectivo é descobrir a chave ou decifrar outros criptogramas.
- Texto limpo escolhido – dispõe-se de um "oráculo" que permite a obtenção de criptogramas para textos escolhidos. O objectivo é decifrar outros criptogramas ou descobrir a chave.
- Criptograma escolhido – dispõe-se de um oráculo para decifrar ciprogramas. Pretende-se obter um criptograma resultante da cifra de um texto limpo determinado.

Viabilidade de ataques por força bruta

Chave	**Tempo** (1µs/test)	**Tempo** (1µs/10^6test)
32 bit	35.8 min.	2.15 msec.
40 bit	6.4 dias	550 msec.
56 bit	1140 anos	10 horas
64 bit	~500000 anos	107 dias
128 bit	$5*10^{24}$ anos	$5*10^{18}$ anos

Técnicas criptográficas a estudar...

- Cifras simétricas
- Cifras assimétricas
- Funções de Hash criptográficas
- Códigos de autenticação (MAC)
- Algoritmos de assinatura digital
- ...