Sumário

- Facetas da segurança.
- Ataques à segurança.
- Cifra.
- Criptografia simétrica.
- Criptografia assimétrica.

Facetas da segurança

- Confidencialidade: *impedir um intruso de aceder a infomação confidencial.*
- Autenticidade: *impedir um intruso/utilizador de personifica um outro utilizador autorizado.*
- Integridade: *impedir um intruso de alterar (ou destruir) informação.*
- Disponibilidade: *garantir o acesso à informação por parte dos utilizadores legítimos.*
- Controlo de acesso: *garantir que apenas os utilizadores autorizados acedem aos recursos.*

Confidencialidade

- Tem por objectivo proteger a informação privada.

  Embora por vezes seja socialmente justificável violar a confidencialidade (por exemplo, para combater o crime organizado).

- Pode ser obtida:

  Impedindo o acesso à informação.

  Cifrando a informação.

Autenticidade

- A informação foi produzida por quem?

  Ter a certeza de quem foi o produtor da informação.

- Impedir a repudiação:

  Quem produziu a informação (ficheiro, mensagem) não poderá negar a sua autoria.

Integridade

- Evitar e ou detectar o forjamento ou alteração de informação (documentos ou mensagens).

  Exemplo: garantir que uma mensagem não pode ser alterada no seu percurso até ao destinatário.

Disponibilidade

- Evitar acções que inpeçam o acesso à informação.

  Bloqueamento, destruição de serviços sensíveis.

  Bloqueamento da comunicação.

- Necessário redundância.

  Nas redes e nos servidores.

Ataques à segurança

- Interrupção de serviço.

  Destruição ou anulação de um recurso.

- Intercepção de informação.

  Cópia de dados, escutas na comunicação.

- Modificação.

  Alteração de dados ou de mensagens.

- Fabricação:

  Inserção de mensagens na rede, adição de entradas em ficheiros.

Tipos de ataques

- Ataques passivos:

  Leitura de conteúdo.

  Análise de padrões na comunicação.

- Ataques activos:

  Personificação; repetição de mensagens; modificação de mensagens; interrupção de serviço.

Criptografia (classificação)

- Operações usadas para cifrar:

  Substituição e transposição.

- Número de chaves:

  Simétrica ou assimétrica.

- Tipo de processamento:

  Por blocos ou por fluxo.

Cripto-análise

- Tentar descobrir o texto original e a chave com base no algoritmo de cifra e:

  No texto cifrado.

  No texto original e no texto cifrado.

  Em sequências escolhidas de texto original (e/ou) cifrado.

- O esforço/tempo necessário para decifrar deve:

  Exceder o valor ou a data de validade da informação.

Tempos de procura exaustiva

Tamanho da chave	Número de chaves	1 Cifra/μs	10^6 Cifras/ μs
32 bits	$4.3x10^9$	35.8 min	1.25 ms
56 bits (DES)	$7.2x10^{16}$	1142 anos	10.01 h
128 bits	$3.4x10^{38}$	$5.3x10^{24}$ anos	$5.4x10^{18}$ anos

Nota: é necessário reconhecer o texto original.

Técnicas de criptografia para texto

- Cifra de césar.

  Transforma uma letra na nª letra que a segue no alfabeto.

- Transposição simples.

  Arranjar uma chave de 26 letras obtida por permutação do alfabeto e transformar o texto de acordo com a chave.

Substituição (tabela de Vigenère)

```
  a b c d e f g h ....
a A B C D E F G H ....
b B C D E F G H I ....
c C D E F G H I J ....
d D E F G H I J K ....
e E F G H I J K L ....
f F G H I J K L M ....
g . . . . . . . . ....
```


Substituição (um exemplo)

```
chave:     umachave
texto:     umafrase
cifrado:   oyahyani
```

Fragilidade: estrutura da lingua (percentagem relativa de utilização de uma dada letra).

Transposição (um exemplo)

```
chave:  4 1 5 2 3
texto:  u m a f r
        a s e q u
        a l q u e
cifrado:mslfqurueuaaaeq
```

O resultado de uma transposição pode ser sujeito a nova transposição, dificultando a cripto-análise.

Para informação binária

- Função de cifrar (E) e de decifrar (D).
- Uma chave para cifrar e outra (possivelmente a mesma) para decifrar.

  E(chave1, dados)= dados cifrados.

  D(chave2, dados cifrados) = dados.
- Deve ser feito de modo a:

  Não ser fácil obter os dados a partir dos dados cifrados sem saber a chave2. Conhecendo os dados e os dados cifrados não deve ser fácil descobrir a chave1.

Criptografia simétrica

- A mesma chave é usada para cifrar e decifrar.
- Existem algoritmos para cifrar com grande eficiencia.
- Fica comprometida se a chave é descoberta.
- É necessário que os dois participantes conheçam a chave.

Data encryption standard (DES)

- Cifra blocos de 64 bits com uma chave de 56 bits.
- A cifra é feita usando uma sequência de 16 iterações de substituição e transposição.
- Pode ser usado em quatro modos diferentes.

DES: modos de operação

- Electronic Codebook (EBC): *dada bloco cifrado de modo independente.*
- Cipher Block Chaining (CBC): *cada bloco é somado (XOR) ao resultado da cifra do bloco anterior antes de ser cifrado.*
- Cypher Feedback mode (CFB)e Output Feedback Mode (OFB): *cifra blocos de oito bits, usando realimentação.*

IDEA

- Proposta de algoritmo para substituir o DES.

  Desenvolvido por Xuejia Lai and James Massey do Swiss Federal Institute of Technology.
- Baseado em chaves de 128 dígitos e cifrando também blocos de 64 dígitos.
- Podem-se usar os mesmos modos de operação que o DES.

Clipper/SKIPJACK

- Proposta do governo federal para um esquema de cifra que:

  Permite a transferência de informação confidencial entre os utilizadores e permite ao sistema legal decifrar a informação se necessário.

- Cada circuito de cifra usa uma chave pública constante e numa chave simétrica variável.
- A cada chave pública estão associadas duas chaves que permitem decifrar qualquer mensagem produzida pelo circuito correspondente.

  Estas chaves são guardadas por agências independentes que as podem fornecer quando justificado.

Criptografia assimétrica

- As chaves são diferentes.

  Tipicamente uma chave é conhecida e a outra é secreta.

  Chave pública e chave privada.

- É necessário: *que não seja fácil encontrar uma chave dada a outra.*
- É útil: *que se possa cifrar com qualquer uma das chaves (e decifrar com a outra).*

Criptografia assimétrica: historial

- Método originalmente proposto em 1976 por Whitfield Diffie e Matin Hellman (Standford Univ.).
- Vários algoritmos para aplicar o princípio.
- O mais conhecido e aceite foi proposto por Ron Rivest, Adi Shamir e Len Adleman (MIT), sendo conhecido por RSA.

Criptografia assimétrica: função

- Não usa substituição e transposição mas sim funções matemáticas.
- Função designada por "trapdoor one-way function"

  $Y = f_k(X)$ *fácil, conhecendo* k *e* X.

  $X = f_k{-}1(Y)$, *improvável, sem conhecer* k.

  $X = f_k{-}1(Y)$ *fácil, conhecendo* k *e* Y.

Notas acerca da criptografia assimétrica

- Pretende evitar a necessidade de um servidor de autenticação que conhece as chaves secretas de dois participantes.
- Não é inerentemente mais segura que a cifra simétrica.

  Depende do comprimento da chave.
- Desvantagem: *é muito mais lento que a chave simétrica.*

Desempenho (rapidez)

Operação	H/W, bit/s	S/W, bit/s/MIP
assimétrica cifrar (RSA)	220 K	.5 K
assimétrica decifrar (RSA)	-	32K
simétrica (DES)	1.2 G	400K
digest (MD4)	-	1300K

Confidencialidade com criptografia assimétrica

- O remetente envia uma mensagem cifrada com a chave pública do destinatário.
- O destinatário é o único que pode decifrar a mensagem com a sua chave secreta.

  Sejam L_s e L_p as chaves secreta e pública do receptor.

  D(L_s, E(L_p, dados)).

Autenticidade com criptografia assimétrica

- O remetente envia uma assinatura cifrada com a sua chave secreta.
- Só a sua chave pública é que consegue reconstruir a sua assinatura.
- O destinatário usa a chave pública do remetente para verificar a assinatura.

  Sejam K_s e K_p as chaves secreta e pública do emissor.

  D(K_p, E(K_s, assinatura)).

Confidencialidade e autencidade

- O remetente assina a mensagem, cifra com a sua chave secreta e cifra o resultado com a chave pública do destinatário.
- O destinatário decifra tudo com a sua chave secreta e autentica-a com a chave pública do remetente.

  $D(K_p,\ D(L_s,\ \underline{E(L_p,E(K_s,\ dados))})))$.

Distribuição das chaves públicas

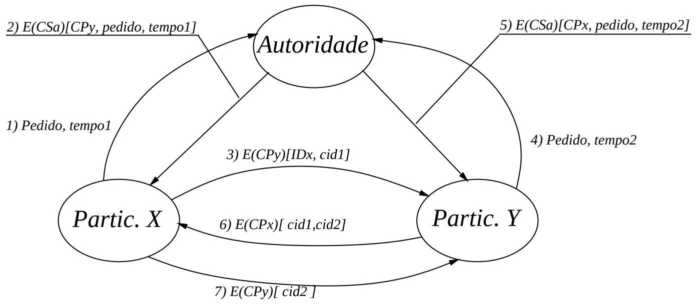
- Anúncio público.

  Problema: falsos anúncios.
- Baseado em directório público.

  Inscrição no directório e sua consulta devem utilizar meios seguros.
- Baseado em autoridade pública.

  Semelhante ao anterior mas usando mensagens cifradas entre os participantes e o directório.

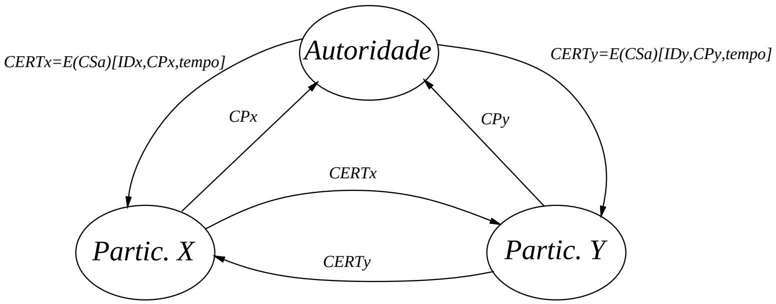
Distribuição de chaves públicas



Certificados de chave pública

- A mensagem gerada pela autoridade, contendo a identificação de um participante e a sua chave pública pode ser usada para certificar a chave pública.
- O certificado pode ser usado para distribuir a chave pública própria ou de outro participante.
- Quem recebe o certificado, usa a chave pública da autoridade para confirmar a sua veracidade.

Distribuição de certificados



Resumo

- Facetas da segurança.

  Confidencialidade, autenticidade, integridade, disponibilidade.

- Ataques à segurança.
- Cifra clássica.

  Substituição e transposição.

- Cifra com chave simétrica.
- Cifra com chaves assimétricas.

  Confidencialidade, autenticação e distribuição de chaves.