Conceitos fundamentais na comunicação:

Confidencialidade;
Autenticação: B tem a garantia de que a mensagem provém de A;
Integridade: B tem a garantia de que a mensagem que recebeu foi aquela que A enviou, sem alterações;
Não repúdio: O emissor não pode, mais tarde, negar que enviou a mensagem;

Cifras simétricas vs assimétricas

Hoje em dia têm-se chaves de 128 bits, para que haja 2^{128} possíveis chaves e o atacante não pode descobrir com facilidade
Simétrica: As chaves de cifragem e decifragem são iguais. Os interlocutores partilham uma mesma chave, que tem de ser previamente acordada e mantida secreta. Neste caso a chave chama-se chave secreta.
Assimétrica: As chaves de cifragem e decifragem são diferentes. Apenas a chave de decifragem precisa de ser secreta, e apenas o recetor a pode conhecer. Um intruso pode conhecer a chave de cifragem, sem que isso comprometa a segurança da cifra.

Electronic Code Book Mode (ECB)

Segurança:
Os padrões existentes no texto limpo não são disfarçados.
Um bloco cifrado duas vezes com a mesma chave resulta em criptogramas iguais.
Suscetível a ataques por code book (compilação de pares texto limpo/criptograma).
Suscetível a ataques por remoção, troca e repetição de blocos.
Eficiência:
Permite o acesso aleatório a dados cifrados.
Qualquer bloco pode ser decifrado independentemente.
Pela mesma razão, permite o processamento paralelo da informação.
Não há possibilidade de efetuar pré-processamento.
Tolerância aos erros:
Este modo não apresenta problemas de propagação de erros entre blocos.
Um erro afeta apenas um bloco de texto limpo.
Erros de sincronização (perda de bits) são irrecuperáveis.

Cipher Block Chaining Mode (CBC)

Necessita de vector IV
Segurança:
Os padrões do texto limpo são mascarados pelo XOR.
De textos limpos iguais passam a resultar criptogramas distintos: impede ataques por code book e por repetição.
Ataques por manipulação de blocos são detetáveis.
Eficiência:
Qualquer bloco pode ser decifrado independentemente, desde que se conheça o bloco anterior.
Pela mesma razão, permite o processamento paralelo da informação cifrada (não aplicável na cifragem). No entanto, uma alteração ao texto limpo, e.g. num ficheiro, implica uma nova cifragem completa.
Permite o acesso aleatório a dados cifrados.
Não há possibilidade de efetuar pré-processamento.
Tolerância aos erros:
Um erro num bit do criptograma afeta o bloco de texto limpo correspondente, e um bit no bloco seguinte.
Erros de sincronização (perda de bits) são irrecuperáveis.

Cipher Feedback Mode (CFB)

Necessita de vector IV
Segurança
Os padrões do texto limpo são mascarados pela pseudo-aleatoriedade da sequência de chaves.
A alteração do IV é determinante. Como em todas as cifras sequenciais, a repetição de uma sequência de chaves torna a cifra vulnerável a ataques.
Eficiência
Qualquer bit pode ser decifrado independentemente, desde que se conheça um número suficiente de bits anteriores do criptograma. Permite o acesso aleatório a dados cifrados.
Pela mesma razão, permite o processamento paralelo da informação cifrada (não aplicável na cifragem).
Há possibilidade de efectuar algum pré-processamento dos bits da chave.
Tolerância aos erros
Erros de sincronização (perda de bits) são recuperáveis em determinadas condições (quais?): é uma cifra auto-sincronizável.
Um erro no criptograma tem como efeito imediato uma decifragem errada do bit de texto limpo correspondente.
Enquanto o bit errado estiver no shift-register, o sistema vai debitar lixo.

Output Feedback Mode (OFB)

Necessita vector IV

Segurança:

Os padrões do texto limpo são mascarados pela pseudo-aleatoriedade da sequência de chaves.
Como no caso anterior, a alteração do IV é determinante.

Eficiência:

Não faz sentido falar de processamento paralelo, uma vez que a sequência de chaves não depende do criptograma.
É possível efetuar a geração de chaves antecipadamente, pelo que a cifragem pode tornar-se muito eficiente.

Tolerância aos erros:

Neste modo não há propagação de erros. Um erro no criptograma afeta apenas um bit no texto limpo.

Escolha de um modo de funcionamento

O **ECB** é muito utilizado para cifrar pequenas parcelas de informação aleatórias, e.g. chaves. Para este tipo de informação as falhas de segurança deste modo não são relevantes.
O **CBC** é o modo de funcionamento recomendado para aplicações genéricas. É muito utilizado para cifrar ficheiros, onde os erros são pouco frequentes. É a melhor escolha para aplicações baseadas em *software*.
O **CFB** e o **OFB** servem para aplicações onde é necessária uma cifra sequencial.
O **OFB** é preferido quando o meio de transmissão introduz muitos erros.

Chaves de Sessão

Esta aproximação tem outras limitações que é impossível transpor:

- uma vez que as chaves permanecem válidas durante a atividade do sistema elas estão expostas durante um tempo prolongado.
- se uma chave for corrompida, e isso não for detetado, o canal entre esse par de agentes deixa de ser seguro.

O conceito de chave de sessão resolve estes problemas:

- É gerada uma chave secreta para cada comunicação.
- Esta chave é estabelecida entre emissor e recetor, utilizada naquele instante, e destruída no fim da comunicação.

Funções One-Way:

A ideia central à Criptografia de Chave Pública (Chave de sessão) é a de uma função One-Way: fácil de calcular, mas muito difícil (de preferência impraticável) de inverter.
Um exemplo muito simples de uma função one-way é a exponenciação: é fácil de calcular y^x , mas obter $\log_y y^x$ é muito mais complicado.

Funções One-Way com trapadoor:

- Como qualquer função one-way, f (x) é fácil de calcular.
- Como qualquer função one-way $f^{-1}(f(x))$ é difícil de calcular.

Se for conhecido o segredo k, $f^{-1}(f(x))$; k) é fácil de calcular.
A aplicação deste tipo de função à criptografia é imediata:

- qualquer agente que conheça a função f pode cifrar informação. No entanto, apenas um agente que conheça o segredo k pode efetuar a decifragem.

Funções de Hash Criptográficas:

- Para garantir integridade interessa extrair uma impressão digital não invertível de uma mensagem: obter **um valor que identifique o conteúdo essa mensagem**.
- O que se consegue na realidade é uma identificação probabilística: é provável que o valor de hash tenha sido originado por aquela mensagem.
- Espera-se que uma função de hash criptográfica seja:
  - **Pre-image resistant**. Dado um valor de hash é difícil encontrar uma pré-imagem desse valor.
  - **Second pre-image resistant** ou fracamente livre de colisões. Dado um hash e a mensagem que o originou, é difícil arranjar outra mensagem que origine o mesmo valor.
  - **Collision resistant** ou fortemente livre de colisões. É difícil encontrar duas mensagens que originem o mesmo hash.
- As funções de hash deste tipo podem ser tornadas públicas. A sua segurança está na baixa probabilidade de encontrar duas mensagens com o mesmo valor de hash.

Exemplo de uma Função de Hash: MD4

O MD4 foi desenvolvido, por Ron Rivest, como uma função de hash para aplicações criptográficas que garantisse:
Segurança, no sentido em que o ataque mais eficiente à função de hash é o ataque por força bruta;
Segurança direta, no sentido em que a base da segurança da função de hash não reside em pressupostos de complexidade computacional como sejam a dificuldade em fatorizar um inteiro grande.

Message Authentication Code (MAC)

Um Message Authentication Code (MAC) pode ser visto como uma função de hash criptográfica cujo resultado depende, não só da **mensagem**, mas também de uma **chave secreta.**
Para gerar o MAC é necessário conhecer o **algoritmo** e a **chave secreta**. O mesmo acontece para o verificar.
Aplicações:

- Impressão digital que garante que o checksum da mensagem foi calculado na sua origem.
- Proteção de ficheiros contra ataques de vírus, uma vez que o vírus seria incapaz de produzir um MAC válido para esconder as alterações que introduzisse.
- Com um MAC é possível comprovar a origem da mensagem e a sua integridade, antes de a decifrar.

Assinaturas Digitais

A assinatura manuscrita é há muito utilizada como prova de autoria ou, pelo menos, de concordância com o conteúdo de um documento. A assinatura deve ser:

- **Autêntica**: convence o recetor do documento de que o signatário explicitamente assinou o documento i.e. que conhecia o seu conteúdo, e.g. por ser o seu autor.
- **Não falsificável**: prova que o signatário, e não outra pessoa, assinou o documento.
- **Não reutilizável**: faz parte do documento e não se pode transpor para outro documento.
- Garante da **integridade do documento**: o documento permaneceu inalterado desde que foi assinado.
- **Não repudiável**: o signatário não pode, à posteriori, negar que assinou o documento.

Notas Importantes:

- Nem todos os algoritmos de assinatura são adaptações diretas de cifras assimétrica.
- É muito importante não confundir uma assinatura digital, que confere autenticação com uma cifra assimétrica.
- Deve evitar-se referir as operações de assinar e verificar uma assinatura como cifrar com chave privada ou decifrar com chave pública.
- O objetivo das assinaturas digitais não é conferir confidencialidade: acompanham o documento a que se referem, que pode ou não ser cifrado.

Faz mais sentido assinar um documento antes de ser cifrado

- Se a mensagem não é assinada antes de ser cifrada, pode haver dúvidas quanto ao conhecimento que o signatário tinha do seu conteúdo.
- Um intruso não tem acesso à informação de autenticação, isto é, à assinatura, a não ser que quebre a cifra.
- Um ataque de substituição ou reutilização da assinatura deixa de fazer sentido.

Princípio do Conhecimento Zero

É feita uma pergunta aleatória cuja resposta depende do segredo. Não conhecendo o segredo, é possível acertar na resposta com 50% de probabilidade. Fazendo uma série de perguntas, consegue-se estabelecer a identidade com uma probabilidade de erro arbitrariamente pequena.
Para o protocolo ser verdadeiramente de conhecimento zero, a resposta não pode implicar a transferência de informação da Alice para o Bob que permita a reconstrução do segredo. Note-se que qualquer mecanismo de assinatura digital pode ser utilizado como f (desafio, K_{Alice}).
Paradoxalmente, para valores de t (número de vezes que lança um desafio) elevados o protocolo Schnorr não é de conhecimento zero, uma vez que o Bob pode controlar e para obter uma solução para uma equação em s que não seria capaz de construir sozinho.

Abstract Syntax Notation One (ASN.1)

A ASN.1 por si só não pode ser utilizada diretamente numa implementação, sendo necessárias normas adicionais para definir como é que se codifica essa notação abstrata em sequências de bits:
Basic Encoding Rules (BER) – mecanismo de codificação definido no standard X.209 e que, por permitir obter várias codificações para o mesmo valor, não é conveniente quando é necessária uma codificação sem ambiguidades.
Distinguished Encoding Rules (DER) – subconjunto do BER definido no standard X.509 e que, introduzindo restrições adicionais à codificação, garante uma codificação única para cada valor ASN.1.

Certificados de Chave Pública

- Um Certificado de Chave Pública é uma estrutura de dados que associa uma chave pública a um determinado agente (a uma representação da sua identidade).
- A associação chave/agente é estabelecida por uma entidade terceira, uma Autoridade de Certificação, que assina digitalmente cada certificado, dando autenticidade e integridade a este.
- A utilidade de um certificado depende unicamente da **confiança** depositada na Autoridade de Certificação.
- Um Certificado de Chave Pública é válido durante um período de tempo bem definido. Esse período vem especificado no conteúdo assinado.

(Ver o processo encriptação/desencriptação pag. 16 e 17 cap.II)

Uma PKI (Public Key Infrastructure) é composta por cinco tipos de componentes:
Titulares de Certificados Possuem as chaves privadas e as utilizam para decifrar mensagens e assinar documentos.
Clientes Utilizam a chave pública contida num certificado para cifrar mensagens e verificar assinaturas.
Autoridades de Certificação Emitem e revogam certificados.
Autoridades de Registo Garantem a associação entre chaves públicas e identidades de titulares (são opcionais).
Repositórios Armazenam e disponibilizam certificados e CRLs.

Protocolos de PKI (ver pag.33 Cap. II)

PKI operações possiveis:
Inicialização Processo inicial que permite ao utilizador comunicar com a PKI: toma conhecimento das CAs em que confia e adquire as chaves públicas e certificados correspondentes, gera o seu par de chaves, etc.
Registo Um utilizador dá-se a conhecer a uma CA (diretamente, ou através de uma RA) para que a CA lhe possa emitir um certificado; para isso fornece informação de identificação que deve ser verificada pela CA (RA).
Geração de Par de Chaves Nalgumas implementações, as CAs encarregam-se de gerar o par de chaves.
Certificação A CA recebe a chave pública do utilizador e a sua identificação e emite o respetivo certificado, segundo regras internas.
Publicação de Certificados e CRLs Esta tarefa pode ser feita diretamente pela CA, ou indiretamente por entidades como RAs. Além de colocar os certificados e CRLs em repositórios é muitas vezes necessário fazer estes documentos chegar aos utilizadores finais por outros meios (on-line ou não).
Revogação Quando um certificado é emitido o seu período útil de vida está pré-definido. No entanto, pode haver a necessidade de invalidar o certificado antes do fim desse período por diversos motivos (e.g. um despedimento, o comprometimento da chave privada, etc.). A revogação de certificados faz-se através de CRLs. As CRLs vão ser analisadas em detalhe mais tarde.
Recuperação de um Par de Chaves Nalgumas implementações as CAs armazenam o par de chaves da entidade como back-up e proteção e.g. no caso de uma empresa e os seus empregados. Nestes casos o par de chaves pode ser restaurado em caso de extravio ou danificação do seu suporte.
Atualização de Par de Chaves Todos os pares de chaves precisam de ser alterados, periodicamente por razões de segurança, ou simplesmente porque a segurança da chave privada foi corrompida.
Certificação de CAs Os certificados das CAs chamam-se **cross certificates**. São utilizados para a validação de cadeias de certificados, mas também podem ser utilizados para outros fins e.g. comunicação segura entre uma entidade e a CA.

Políticas de Certificação
Uma CP (Certificate Policies) é um conjunto de regras que define a aplicabilidade de certificados a uma determinada comunidade ou classe de aplicações:
- A legislação em que se baseará a emissão e utilização dos certificados.
- Os requisitos e as responsabilidades (nomeadamente legais e financeiras) associados a CAs (certified authority) e RAs (Root authority).
- Os requisitos e as responsabilidades associados a Titulares e Clientes.
- Restrições ao conteúdo e utilização dos certificados e.g. somas máximas envolvidas numa transacção, etc.
- Procedimentos a serem implementados relativamente adiversos aspectos do funcionamento de CAs e RAs.

Certificate Revocation Lists (CRL)
As Certificate Revocation Lists (CRL) são o canal previsto no X.509 para a revogação de certificados dentro do período de validade.

Sessão SSL
- Caso seja utilizada autenticação do Servidor, este envia o seu certificado X.509 ao Cliente, que o valida. Além da validação habitual, o Cliente assegura-se de que o nome de domínio do Servidor, indicado no certificado, está correto;
- Parâmetros do Servidor específicos para acordo de chaves são enviados nesta fase (**Server Key Exchange**);
- Caso o Servidor autentique o Cliente, solicita o certificado correspondente (**Certificate Request**). Este pedido inclui um desafio para ser utilizado na autenticação do cliente.
- O Servidor termina esta fase da negociação enviando uma mensagem **Server Hello Done**.
- Conjuntamente com o certificado o Cliente tem de enviar uma assinatura digital do desafio que recebeu, comprovando assim a posse da chave privada associada ao certificado.
- Finalmente, o Cliente envia os seus parâmetros para acordo de chaves (**Client Key Exchange**), altera o seu estado de sessão, e envia uma primeira mensagem cifrada que indica o seu estado de prontidão (**finished**).
- O Servidor efectua o mesmo procedimento e a negociação termina tendo sido acordado o Master Secret da sessão.

SSH

Num servidor que utilize o SSH têm de ser definidas as seguintes políticas de segurança:

- Quais os algoritmos de cifragem, compressão e autenticação utilizáveis para envio e recepção de dados; e, desses algoritmos, quais são as soluções preferenciais.
- Quais os algoritmos de Chave Pública utilizados para acordo de chaves e autenticação do Servidor.
- Que tipo de autenticação é requerida aos utilizadores que acedem a partir de um determinado Cliente.
- Quais as operações que um utilizador pode efectuar, dependendo da sessão que estabeleceu.

Servidor Kerberos

Num servidor Kerberos distinguem-se dois serviços: o Authentication Server e o Ticket Granting Server.
A obtenção de uma Credential para aceder a um qualquer Servidor é, geralmente, uma negociação com duas fases:

- O Cliente solicita primeiro uma Credential contendo um Ticket Granting Ticket ao Authentication Server.
- Um Ticket Granting Ticket é um Ticket especial que permite ao Cliente aceder ao Ticket Granting Server de forma segura.
- Utilizando o Ticket Granting Ticket, o Cliente pode obter a Credential que pretende junto do Ticket Granting Server.

Em casos especiais a obtenção do Ticket pode ser feita numa só fase, directamente junto do Authentication Server.