atec

Segurança em Sistemas Informáticos

Formador: Pedro Sardinha

Segurança em Sistemas Informáticos

Objetivos especificos

- Vulnerabilidades, ameaças e ataques
- Políticas de segurança e mecanismos de segurança
- Segurança em sistemas distribuídos
- Conceitos gerais sobre criptografia
- Tipos de cifra
- Criptografia de chave pública
- Gestão de chaves

Segurança?

"Um estado de segurança e livre de perigo ou dano; as ações realizadas para tornar alguém ou algo seguro."

Conceitos gerais sobre segurança da informação

- Uma organização deve possuir múltiplas camadas de segurança para proteger:
  - Operações
  - Infraestrutura física
  - Pessoas
  - Funções
  - Comunicações
  - Informação

Segurança da Informação?

"A proteção da informação e dos seus elementos críticos, incluindo sistemas e hardware que usam, armazenam e transmitem informação" – *Committee on National Security Systems (CNSS)*

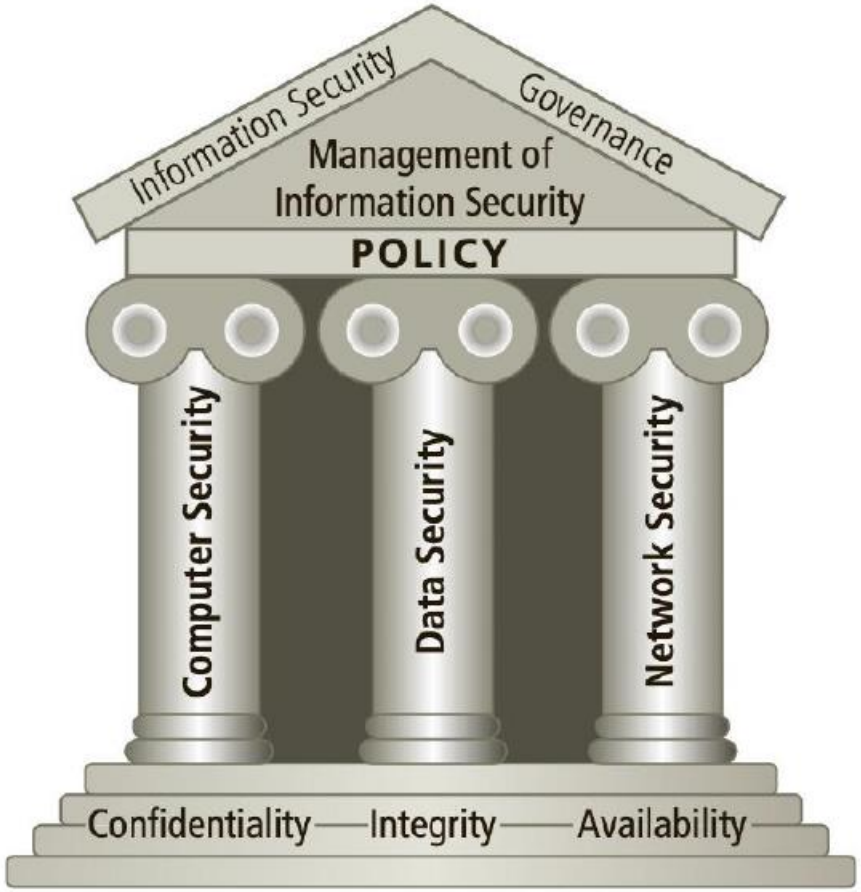
Segurança em Sistemas Informáticos

Segurança da Informação – C.I.A tríade

Segurança da Informação?

- Inclui a gestão da **segurança de informação**, **segurança de dados** e **segurança de redes**.

- Triângulo da **Confidencialidade**, **Integridade** e **Disponibilidade** (C.I.A. tríade)
  - É uma norma que se baseia na confidencialidade, integridade e disponibilidade.



Segurança em Sistemas Informáticos

Conceitos Chave

Conceito	Definição
Acesso	A **habilidade** de um **sujeito** ou **objeto** de **usar**, **manipular**, **modificar** ou **afetar** outro **sujeito** ou **objeto**.
Ativo	O **recurso** organizacional **que está a ser protegido**. Um ativo pode ser **lógico ou intangível**, como um site da Web, informações de software ou dados; ou um ativo pode ser **físico ou tangível**, como uma pessoa, sistema de computador, hardware ou outro objeto tangível.
Ataque	Um **ato intencional** ou **não intencional** que **pode danificar ou comprometer as informações e os sistemas que as suportam**. Os ataques podem ser **ativos** ou **passivos**, **intencionais** ou não **intencionais** e **diretos** ou **indiretos**.
Controlo, Salvaguarda ou Contramedida	**Mecanismos**, **políticas** ou **procedimentos de segurança** que **podem conter ataques**, **reduzir riscos**, **resolver vulnerabilidades** e de outra forma **melhorar a segurança** dentro de uma organização.
"Exploit"	Uma **técnica usada para comprometer um sistema**.
Exposição	Uma **condição** ou **estado** de **exposição**; na segurança da informação, a **exposição existe quando uma vulnerabilidade é conhecida por um invasor**.

Segurança em Sistemas Informáticos

Conceitos Chave

Conceito	Definição
Perda	Uma **instância de um ativo de informação** que **sofra danos ou destruição**, **modificação** ou **divulgação não intencional** ou **não autorizada** ou **negação de serviço**.
Perfil de Proteção ou Postura de Segurança	Todo o **conjunto de controlos e salvaguardas**, incluindo **política**, **educação**, **treino** e **sensibilização**, e **tecnologia**, que a **organização implementa para proteger o ativo**.
Risco	A **probabilidade de uma ocorrência indesejada**, como um **evento adverso ou perda**.
Ameaça	**Qualquer evento ou circunstância** que tem o **potencial de afetar adversamente as operações e ativos**.
Agente da Ameaça	A **instância específica** ou **um componente de uma ameaça**.
Evento da Ameaça	Uma **ocorrência de um evento causado por um agente de ameaça**.
Fonte da Ameaça	Uma **categoria de objetos**, **pessoas** ou **outras entidades** que **representam a origem do perigo para um ativo.**
Vulnerabilidade	Uma **fraqueza potencial num ativo** ou no **sistema de controlo defensivo**.

Segurança em Sistemas Informáticos

Segurança da informação

Segurança em Sistemas Informáticos

Vulnerabilidades, ameaças e ataques

- Vulnerabilidades

    1. Hardware
    2. Software
    3. Humana

Segurança em Sistemas Informáticos

Ameaças - Tipologias

Naturais

- Eventos provocados pela mãe natureza
- Tornado, furacão, terramotos, fogo, inundação, tsunami, tempestade de neve, granizo, entre outros.

Técnicas

- Falha do disco ou servidor, bug ou vulnerabilidade no software, virus, código malicioso, falhas de rede.

Provocadas pelo Homem

- Ataques propositados (hackers), sabotagem, roubo, fraude, greve, revolta, alterações políticas/legais, erros e omissões, engenharia social, etc.

Sistema de Fornecimento

- Electricidade, HVAC, água/esgotos, matérias primas.

Segurança em Sistemas Informáticos

Ameaças - Categorias

Categoria de Ameaça	Exemplo de Ataque
Atos de erros ou falhas humanas	Acidentes, erros de empregados
Compromisso da propriedade intelectual	Pirataria, infração de copyright
Espionagem ou invasão	Acesso não autorizado e/ou coleção de dados
Extorção de informação	Chantagem com informação revelada
Sabotagem ou vandalismo	Destruição de sistemas ou de informação
Roubo	Confiscamento ilegal de equipamento ou informação
Ataques de software	Virus, worms, macros, negação de serviço
Forças de natureza	Fogo, inundações, terramotos, raios
Desvios na qualidade de serviço	Falhas no fornecimento de Internet ou de energia
Erros ou falhas técnicas de hardware	Falha de equipamento
Erros ou falhas técnicas de software	Bugs, problemas de código
Obsolescência tecnológica	Tecnologias antiquadas ou desatualizadas

Segurança em Sistemas Informáticos

Falhas Humanas

- Sem intenções maliciosas

- Causas:
  - Inexperiência;
  - Formação inadequada ou insuficiente;
  - Decisões incorretas.

Principais Ameaças aos dados – Empregados das organizações.

Segurança em Sistemas Informáticos

Falhas Humanas

- Erros podem causar:
  - Revelação de dados confidenciais;
  - Introdução de dados incorretos;
  - Modificação ou remoção acidental de dados;
  - Armazenamento de dados em áreas desprotegidas;
  - Falhas na proteção da informação.

- Social engineering

Vídeo - https://www.youtube.com/watch?v=YAHPGPO3BFo

Segurança em Sistemas Informáticos

Espionagem ou invasão

- Acesso a informação protegida por parte de indivíduos não autorizados.
- Pode acontecer em qualquer lugar em que se aceda à informação confidencial.
- Os atacantes usam suas capacidades para ultrapassar controlos de segurança.

Segurança em Sistemas Informáticos

Roubo

- Obtenção ilegal da propriedade física, eletronica ou intelectual por terceiros
    - Roubo físico
    - Roubo eletrónico

Segurança em Sistemas Informáticos

Ataques de software

- Malware
  - Software malicioso que danifica, destrói ou nega o serviço a determinados sistemas.
- Inclui:
  - Virus
  - Worms
  - Trojan horses
  - Logic bombs
  - Backdoors
  - Ataques DoS

Segurança em Sistemas Informáticos

Tipos de Malware

- Malware
  - Software malicioso que danifica, destrói ou nega o serviço a determinados sistemas.
- Inclui:
  - Virus
  - Worms
  - Trojan horses
  - Logic bombs
  - Backdoors
  - Ataques DoS
  - Ransomware

Video - https://www.youtube.com/watch?v=BMbGdyZiHWU

Segurança em Sistemas Informáticos

Tipos de Malware

- Virus
  - código malicioso executável que está anexado a outro arquivo executável, como um programa legitimo.
  - A maioria precisa de ação do utilizador e da execução de um programa no hospede (computador infectado).

  - Origem
    - Anexo email
    - Word, Excel, etc.
    - Outros arquivos
    - Programas de origem duvidosa
    - Pen drive

Segurança em Sistemas Informáticos

Tipos de Malware

- Worms
  - Programas capazes de se propagar automaticamente através da rede, envia copias de computador para computador.
  - Sobrecarrega a rede.
  - Ao contrário do vírus, não precisa de um hospede para executar.

Segurança em Sistemas Informáticos

Tipos de Malware

- Cavalo de troia (Trojan horse)
  - Programa normalmente recebido como um “presente”.
    - Programa inofensivo, álbum de fotos, jogo, etc
    - Faz a função do programa mas também executa outras normalmente maliciosas e sem consentimento do utilizador.
  - Funções maliciosas:
    - Roubo de senhas ou informação confidencial.
    - Inclusão de Backdoor – permite ao atacante total controle sobre o computador.
    - Acesso, cópia, alteração ou destruição de arquivos.

Segurança em Sistemas Informáticos

Tipos de Malware

- Bombas lógicas
  - Código malicioso que utiliza um gatilho para ativar
    - Podem ser datas, horas, outros programas em execução.

  - Funções maliciosas:
    - Danificar bases de dados.
    - Apagar ficheiros.
    - Atacar sistemas operativos ou programas.
    - Danificar hardware.

Segurança em Sistemas Informáticos

Tipos de Malware

- Ransomware
  - Criptografa os dados no computador com uma chave desconhecida do utilizador.
  - Pede um resgate ao utilizador para desbloquear os dados.

  - Criminoso exige pagamento através de um sistema de pagamento não detetável.
    - Usam bitcoin ou criptomoedas.

Segurança em Sistemas Informáticos

Tipos de Malware

- Backdoors
- Rootkits
- Bots
- Botnets
- Keyloggers
- Spam
- Spyware
- Adware
- Scareware
- Phishing
- DoS (Denial-of-Service)
- DDoS (Distributed DoS Attack)
- Sniffing
- Spoofing
- Man-in-the-middle
- Ataques de Dia Zero
- Keyboard Logging

Segurança em Sistemas Informáticos

Categorias de ameaças

- Forças da natureza
  - Estão entre as ameaças mais perigosas
  - Podem causar disrupções nas vidas dos indivíduos e afetar o armazenamento, transferência e uso de informação.
  - Organizações – devem implementar controlos para limitarem danos e preparem-se para os piores cenários.

Segurança em Sistemas Informáticos

Categorias de ameaças

- Extorsão
  - Acto de um atacante ou de alguém interno à organização que **rouba ou interrompe o acesso à informação** de um sistema informático e **exige uma compensação pela sua devolução** ou por um **acordo de não divulgação** da informação.

  - **Ransomware** (mais conhecido)

Segurança em Sistemas Informáticos

Categorias de ameaças

- Sabotagem ou vandalismo

  - **Sabotagem deliberada** de um **sistema** ou **negócio** informático, ou actos de vandalismo para **destruir um bem** ou **danificar a imagem** de uma organização.

  - Estes actos podem variar **desde pequenos actos de vandalismo** por empregados até à **sabotagem organizada** contra uma organização.

  - Atores:
    - Ciberterroristas/Ciberguerra (Stuxnet)
    - Hacktivismo

Segurança em Sistemas Informáticos

Categorias de ameaças

- Erros ou falhas técnicas de hardware
  - Falhas ou erros técnicos de hardware ocorrem quando um **fabricante** distribui equipamento com uma **falha conhecida** ou **desconhecida.**
  - Estes **defeitos** podem fazer com que o **sistema funcione fora dos parâmetros esperados**, resultando num serviço **pouco fiável** ou na **falta de disponibilidade**.
  - Algums erros são terminais – perda irrecuperável do equipamento.
  - Outros são intermitentes – manifestam-se periodicamente, resultando em falhas que não são facilmente repetidas.

Segurança em Sistemas Informáticos

Categorias de ameaças

- Erros ou falhas técnicas de software
  - Grandes quantidades de código são escritas, depuradas, publicadas e vendidas antes de todos os seus **bugs serem detectados e resolvidos**.
  - Por vezes, combinações de determinado software e hardware **revelam novas falhas que variam desde bugs a condições de falha não testadas.**

1. SQL injection
2. Web server- and client-related vulnerabilities
3. Use of magic URLs, predictable cookies, and hidden form fields
4. Buffer overruns
5. Format string problems
6. Integer overflows
7. C++ catastrophes
8. Insecure exception handling
9. Command injection
10. Failure to handle errors
11. Information leakage
12. Race conditions
13. Poor usability
14. Not updating easily
15. Executing code with too much privilege
16. Failure to protect stored data
17. Insecure mobile code
18. Use of weak password-based systems
19. Weak random numbers
20. Using cryptography incorrectly

Segurança em Sistemas Informáticos

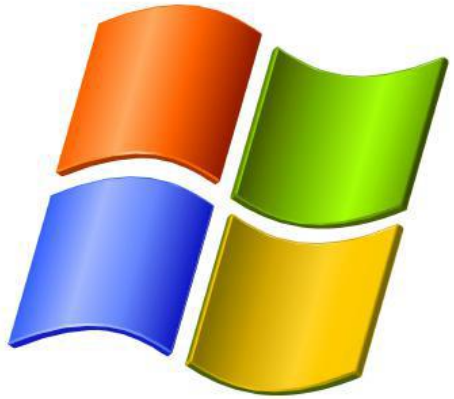
Categorias de ameaças

- Desvios na qualidade de serviço
  - Acesso à internet
  - Comunicações
  - Fornecimento de energia

Segurança em Sistemas Informáticos

Categorias de ameaças

- Obsolescência tecnológica
    - Infraestruturas antiquadas e desatualizadas.



Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- **Dentro de uma organização**, os profissionais de segurança da informação **ajudam** a **manter a segurança** através do **estabelecimento e aplicação de políticas**.
- Estas **políticas** funcionam **como leis organizacionais**, completas com **sanções**, **práticas judiciais**, e **diretrizes para exigir o seu cumprimento**
- **Políticas**: directivas de gestão que **especificam** o **comportamento aceitável** e inaceitável dos **trabalhadores** no local de trabalho
- As políticas **funcionam como leis organizacionais**; devem ser elaboradas e implementadas com cuidado para **garantir que são completas, apropriadas e aplicadas de forma justa a todos**.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- **Politica de Segurança**
  - Objetivo – proteção das informações da empresa e implementada através dos princípios básicos:

    - **Confidencialidade**
    - **Integridade**
    - **Disponibilidade**

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- As regras e procedimentos são normalmente definidos num documento, regulando:
    - A utilização de computadores e outros dispositivos
    - A utilização da Internet (ex. não é permitido o download de torrents ou streaming)
    - A utilização de serviços disponibilizados pela empresa
    - restringindo a instalação de aplicações ou alteração de parâmetros associados aos perfis de cada utilizador
    - Definição de cronogramas de backup
    - Estabelecimento de regras para o uso de senhas e credenciais de acesso
    - Controlo de acesso aos espaços físicos
    - Criação de planos de contingência e de gerenciamento de riscos
    - Definição de politicas de atualização de softwares.

Além da definição de regras e procedimentos, esse documento deve também incluir procedimentos disciplinares no caso da violação das regras definidas na política de segurança informática da empresa.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

1. Declaração da política
   a) Âmbito e aplicabilidade
   b) Definição das tecnologias abordadas
   c) Responsabilidades
2. Acesso autorizado e utilização de equipamento
   a) Acesso de utilizadores
   b) Uso responsável e justo
   c) Proteção da privacidade
3. Uso proibido de equipamento
   a) Uso disruptivo ou mau uso
   b) Uso criminoso
   c) Materiais ofensivos ou de assédio
   d) Materiais protegidos por copyright, licenciados ou outro tipo de propriedade intelectual
   e) Outras restrições
4. Gestão de Sistemas
   a. Gestão de materiais armazenados
   b. Monitorização de empregados
   c. Proteção de virus
   d. Segurança física
   e. Encriptação
5. Violações de política
   a) Procedimentos para reportar violações
   b) Penalidades por violações
6. Revisões e modificações da política
   a) Revisão programada dos procedimentos para a modificação das políticas
   b) Declaração de limitações de responsabilidade legais
7. Limitações de responsabilidade
   a) Declarações de responsabilidade
   b) Outras declarações de limitações de responsabilidade se necessário

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Autenticação
  - As passwords devem ser constituídas no mínimo por 9 caracteres:
    - Letras minúsculas (a, b, c, ... z);
    - Letras maiúsculas (A, B, C, ... Z);
    - Números (0, 1, 2, ... 9);
    - Caracteres especiais (~ ! @ # $ % ^ & * ( ) _ + | ` - = \ { } [ ] : " ; ' < > ? , . /).

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Autenticação
  - Manter as palavras-passe confidenciais;
  - Memorizar as palavras-passe e não escrever em papeis ou locais visíveis;
  - Mudar regularmente as palavras-passe, mesmo que o sistema não o obrigue a fazer;
  - Utilizar cifras para guardar as palavras-passe;
  - Não utilizar as mesmas palavras-passe para os sistemas laborais e sistemas pessoais;
  - Utilizar palavras-passe fáceis de memorizar;
  - Para criar uma palavra-passe segura, pense primeiro numa frase fácil de memorizar e depois defina um método para transformar a frase numa palavra-passe.

Frase: eu comprei o meu primeiro carro em 2017!
Método: primeira letra de cada palavra, alternar irregularmente entre letra maiúscula e minúscula, usar apenas os últimos dois algarismos de números e manter caracteres especiais.
Palavra-passe: EcoMPcE17! (Não utilize este exemplo)

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Configurações seguras
  - Utilize software obtido apenas de fontes legítimas e mantenha-o sempre atualizado;
  - Altere passwords pré-definidas e, se for necessário, as configurações originais (default);
  - Não continue a usar software que já não seja suportado pelo fornecedor.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Dispositivos móveis externos
  - Duvide de dispositivos externos (memórias USB, etc.) com origem desconhecida;
  - Desative a funcionalidade de arranque automático (autorun);
  - Antes de aceder a qualquer ficheiro, analise-o com um antivírus.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Email
  - Criação de conta de correio eletrónico institucional para comunicação eficaz e desmaterializada. Este endereço é o meio privilegiado de contacto, sendo equiparado às formas tradicionais de comunicação oficial, pelo que não deve ser substituído por soluções externas.

  - A utilização do correio eletrónico está condicionada por uma Política de Utilização Aceitável, que inclui o respeito pelos direitos dos restantes utilizadores, assim como o cumprimento de obrigações legais.

  - Assegurar o normal funcionamento deste serviço em termos de conetividade, monitorização e integridade da informação. Apesar de nas caixas de entrada ainda surgir um volume considerável de spam, a maioria das mensagens deste tipo são eliminadas pelos filtros de entrada.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Email
  - Criação de conta de correio eletrónico institucional para comunicação eficaz e desmaterializada. Este endereço é o meio privilegiado de contacto, sendo equiparado às formas tradicionais de comunicação oficial, pelo que não deve ser substituído por soluções externas.

  - A utilização do correio eletrónico está condicionada por uma Política de Utilização Aceitável, que inclui o respeito pelos direitos dos restantes utilizadores, assim como o cumprimento de obrigações legais.

  - Assegurar o normal funcionamento deste serviço em termos de conetividade, monitorização e integridade da informação. Apesar de nas caixas de entrada ainda surgir um volume considerável de spam, a maioria das mensagens deste tipo são eliminadas pelos filtros de entrada.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Email
  - Segurança
    - As mensagens podem ser assinadas digitalmente (via Certificado Digital, como por exemplo o do Cartão de Cidadão), de forma a melhorar a confiança do recetor no remetente;
    - O envio de dados críticos/sensíveis por correio eletrónico só deve ser feito se tal for requerido pelas funções desempenhadas, sendo neste caso obrigatório encriptar a mensagem;
    - Os utilizadores devem proteger-se dos ataques de phishing rejeitando qualquer mensagem que não lhes seja diretamente remetida, que contenha assuntos não solicitados ou que levante dúvidas. Nunca se deve fornecer informação pessoal ou credenciais do serviço;
    - Faça pairar o rato sobre qualquer apontador embebido na mensagem recebida para confirmar se correspondem ao texto visível, antes de seguir as respetivas ligações;
    - Não abra anexos que terminem em .exe, .scr, .bat, .com, ou outros ficheiros executáveis que não sejam de confiança ou levantem dúvidas.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Email
  - Cuidados adicionais
    - Não use o correio eletrónico para divulgar publicidade, especialmente para contactos que não o solicitaram.
    - Partilhe uma mensagem com terceiros, em Cc (carbon copy, conhecimento de terceiros com endereços visíveis) ou Bcc (blind carbon copy, conhecimento de terceiros com endereços ocultos), apenas quando essas pessoas efetivamente necessitarem da informação;
    - Utilize o Reply All com parcimónia, pois ninguém gosta de encher a caixa de entrada com mensagens e agradecimentos que não lhe sejam dirigidos.
    - Utilize o Forward para partilhar uma mensagem com outrem se quiser continuar a acompanhar o assunto, e o Redirect se o assunto não lhe disser respeito.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Impressões
  - Deve recolher as impressões o mais rápido possível da impressora. Se imprimir documentos com dados sensíveis, faça o acompanhamento presencial da saída das folhas.
  - Se quiser destruir documentação com informação importante (por exemplo, dados pessoais), recorra a procedimentos fidedignos como a trituração.
  - Se possível, usar dispositivos de impressão com PIN ou outra forma de autenticação (impressão segura)

Politicas de Segurança e mecanismos de seguranças

- Incidentes de Segurança da Informação
  - Se ocorrer uma situação anormal que pode pôr em causa os seus recursos (perda de um dispositivo, infeção com vírus, suspeita de violação das suas credenciais, destruição acidental de dados pessoais, etc.)
  - Canal de reporte de incidente de segurança – equipa com endereço de email.

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças

- Prevenção de Malware
  - Instalar e manter atualizado o antivírus (defesa contra código malicioso).
- Utilização
  - Não abra ficheiros cuja origem não lhe garanta confiança;
  - Não aceda a links de origem desconhecida - pare e analise-os antes de se conectar;
  - Não utilize o seu equipamento de trabalho para fins pessoais;

O Phishing trata-se de um crime informático baseado no envio de um email fraudulento com o objetivo de obter dados pessoais ou de negócio. É um email falso, normalmente emitido em nome de uma entidade credível tal como um Banco, Facebook, Twitter, Microsoft, Vodafone, etc. mas que na realidade só pretende recolher dados ou infetar os sistemas.

Segurança em Sistemas Informáticos

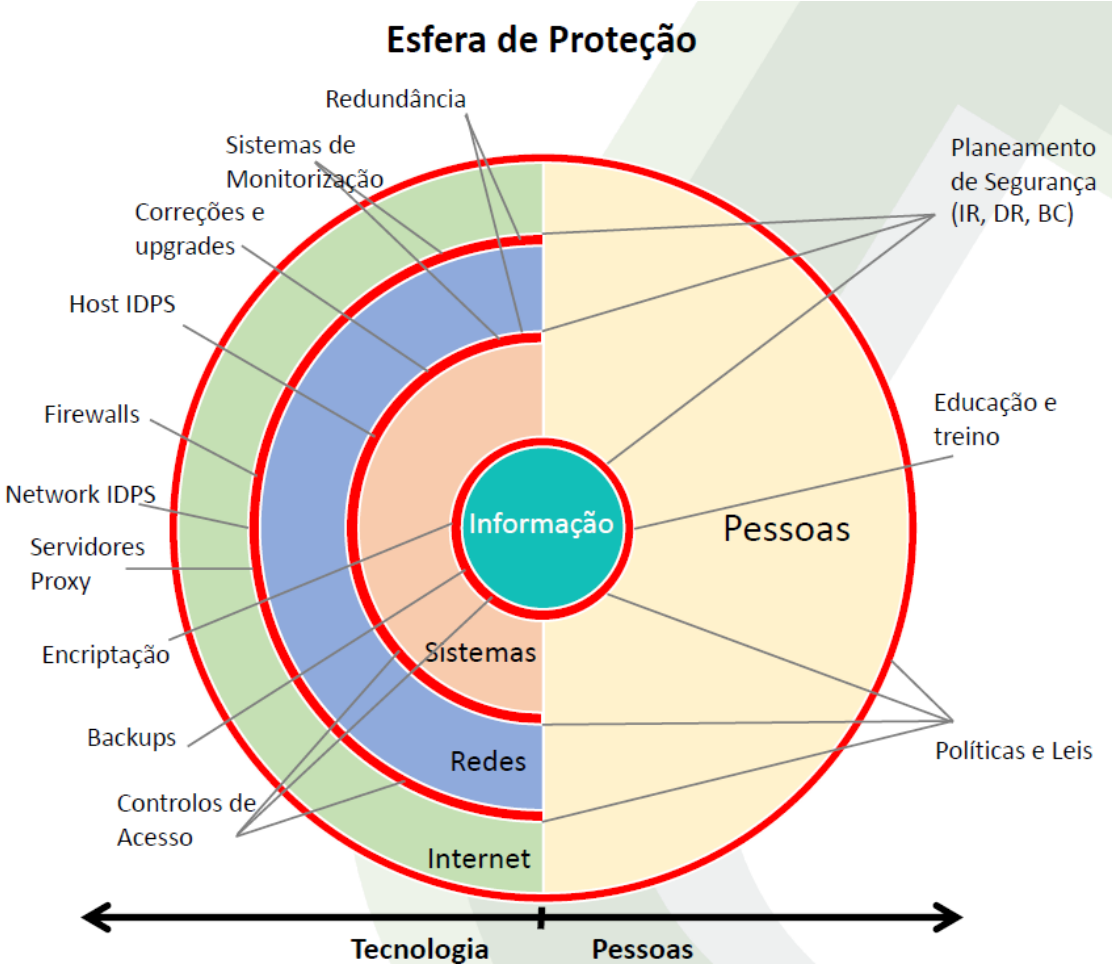
Politicas de Segurança e mecanismos de seguranças

- Redes Wi-fi
  - Evite conetar-se a redes Wi-Fi sem autenticação ou de entidades desconhecidas. Se não puder evitar, adote medidas de autoproteção:

    - Utilize uma VPN;
    - Não aceda a serviços críticos;
    - Certifique-se de que os sites a que acede são seguros fazendo duplo clique sobre o cadeado que aparece no seu browser junto à área do endereço Web do site (que deve começar por "https://" e não por "http://“).

Segurança em Sistemas Informáticos

Politicas de Segurança e mecanismos de seguranças



- Firewalls
- Redundância
- Sistemas de Monitorização
- Correções e upgrades
- Backups
- Pessoas

Segurança em Sistemas Informáticos

Segurança em sistemas distribuidos

- Sistemas Confiáveis?
  - Área da informática que estuda os problemas e as soluções inerentes à realização de sistemas seguros e fiáveis – **de confiança.**
    - Deverá exibir diversas propriedades:
      - Disponibilidade, fiabilidade perante falhas
      - Redundância, replicação e seguro perante ataques.
    - **Como ?**
      - Politicas (regras) de segurança suportadas por mecanismos de segurança, implementadas sobre uma base de confiança estabelecida à partida.

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Sistemas distribuídos são suscetíveis a novos tipos ataques...
- A separação física dos componentes (e a necessidade de comunicarem entre si, através de uma rede) introduz **vetores de ataque** adicionais.
- É necessário uma reavaliação da base de confiança -> **trusted computing base**.
- Para implementar políticas de segurança equivalentes, são necessários mecanismos de segurança mais sofisticados face a um sistema isolado.

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Modelo de Segurança

  - Num sistema existem entidades que do ponto de vista da segurança têm identidade própria, direitos e deveres - essas entidades podem ser utilizadores, componentes, processos, etc. e designam-se pelo termo **principal**

  - A segurança do sistema distribuído passa por:
    - autenticar os principais (**autenticação**)
    - verificar os seus direitos de acesso aos objetos (**controlo de acessos**)
    - da distribuição advém a necessidade de utilizar canais seguros para impedir o acesso, alteração ou destruição indevida de informação, incluindo, **proteger a privacidade**

  Para fornecer segurança é necessário estabelecer que alguns componentes do sistema são seguros (**trusted computing base**) – caso contrário é impossível

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Elementos do Modelo de Segurança

Principal - uma entidade (pessoa, processo, servidor, cliente, …) que é singular do ponto de vista dos direitos no sistema.

Autenticação – processo de verificar que um principal P tem a identidade que diz ter – em geral, deve ser capaz de o provar.

> Geralmente utiliza-se um método lógico do tipo segredo partilhado entre P e quem o autentica (de que uma palavra chave é o exemplo mais conhecido), mas também se pode basear na verificação de atributos físicos (identificação da voz, impressões digitais ou da retina por exemplo) ou na posse de algo que só P pode possuir (um cartão magnético por exemplo).

Controlo de acessos - dada uma operação Op sobre um objecto O, é necessário decidir se o principal P pode aplicar Op a O.

- Camadas de Segurança

A segurança de um sistema pode ser endereçada por camadas.

O papel de cada camada é estabelecer uma linha de defesa e alargar a trusted computing base para as camadas superiores.

A base de confiança (trusted computing base) inicial deve ser tão minimalista quanto o possível uma base de confiança reduzida à partida tem uma superfície de ataque mais reduzida .

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Vetores de Ataque usuais

Adulterar a base de confiança computacional (trusted computing base - TCB)

Explorar insuficiências na trusted computing base

Falhas na especificação ou implementação da TCB podem dar ao atacante direitos ou identidades indevidas.

Violar os mecanismos de autenticação

Obter segredos indevidos

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Vetores de Ataque usuais

Os ataques são muito diversos, podem ser muito engenhosos...

Exploram bugs, insuficiências das implementações ou de planeamento ou simples fraquezas humanas...

Na prática, **é impossível de enunciar todas as formas de ataque** e quase sempre estão-se a descobrir novas.

A tarefa de manter os sistemas seguros é um esforço contínuo que envolve todos.

Há programas de recompensam a descoberta de problemas de segurança em produtos de grande consumo.

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Vetores de Ataque usuais

Os ataques são muito diversos, podem ser muito engenhosos...

Exploram bugs, insuficiências das implementações ou de planeamento ou simples fraquezas humanas...

Na prática, **é impossível de enunciar todas as formas de ataque** e quase sempre estão-se a descobrir novas.

A tarefa de manter os sistemas seguros é um esforço contínuo que envolve todos.

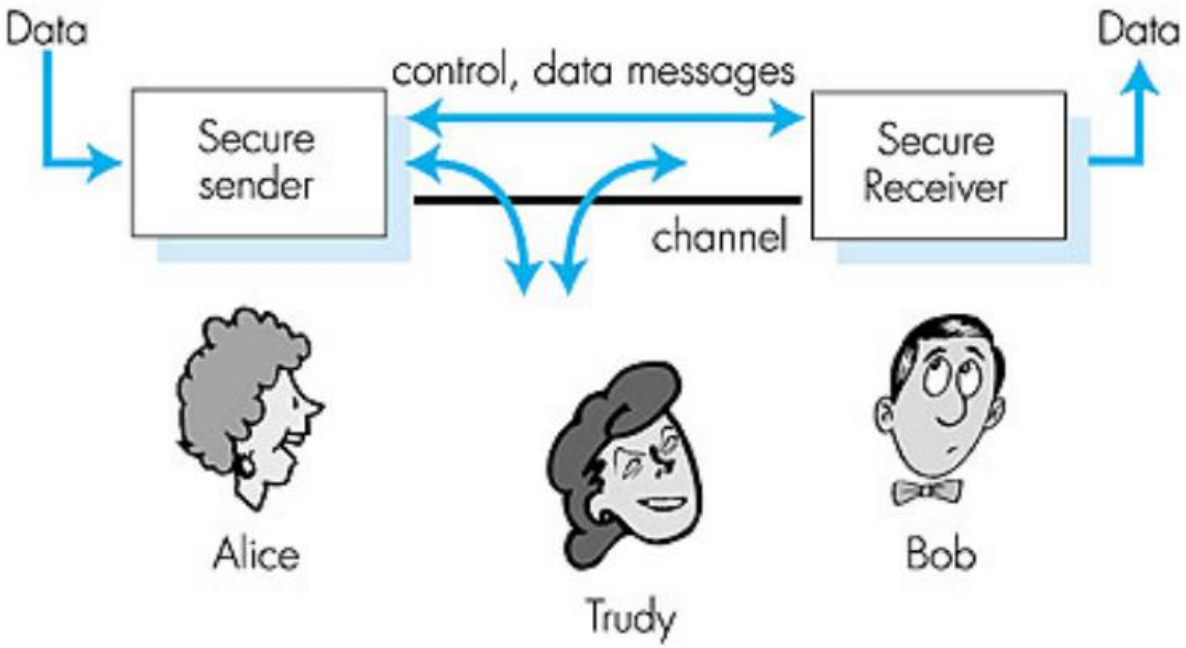
Há programas de recompensam a descoberta de problemas de segurança em produtos de grande consumo.

BUG BOUNTY HUNTERS

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Comunicação num sistema sem segurança



Canal está acessível ao atacante.

Nomes usados na descrição dos protocolos de segurança:

Alice, Bob, Carol, Dave – participantes que querem comunicar
Eve é usado para um atacante que lê mensagens – eavesdropper)
Mallory/Trudy – atacante que pode ler, interceptar, modificar, suprimir ou re-introduzir mensagens nos canais ou tentar passar por um dos participantes
Sara – um servidor.

Segurança em sistemas distribuídos

- Ataques em sistemas distribuídos através da comunicação

Indiscrição – obtenção de mensagens sem autorização (Eavesdropping)
Mascarar-se ou **pretender** ser outro (Masquerading)
Reemissão de mensagens prévias (Message replaying)
Adulteração do conteúdo das mensagens (Message tampering)
Supressão de mensagens (Message supression)
Vandalismo por impedimento de prestação de serviço (Denial of service attacks)
Repúdio de mensagens, negar a autoria de mensagens
Análise de tráfego (Traffic analysis) procurando padrões que possam indiciar a natureza da comunicação, dos protocolos, etc.

Segurança em sistemas distribuídos

- Ataques em sistemas distribuídos através da comunicação

Indiscrição – obtenção de mensagens sem autorização (Eavesdropping)
Mascarar-se ou **pretender** ser outro (Masquerading)
Reemissão de mensagens prévias (Message replaying)
Adulteração do conteúdo das mensagens (Message tampering)
Supressão de mensagens (Message supression)
Vandalismo por impedimento de prestação de serviço (Denial of service attacks)
Repúdio de mensagens, negar a autoria de mensagens
Análise de tráfego (Traffic analysis) procurando padrões que possam indiciar a natureza da comunicação, dos protocolos, etc.

- Defesa

Mecanismos de segurança mais comuns
Recurso à criptografia para:

obter **canais seguros**, imunes à repetição e violação da integridade dos dados e garantir confidencialidade

autenticar os principais (utilizadores, servidores, etc)

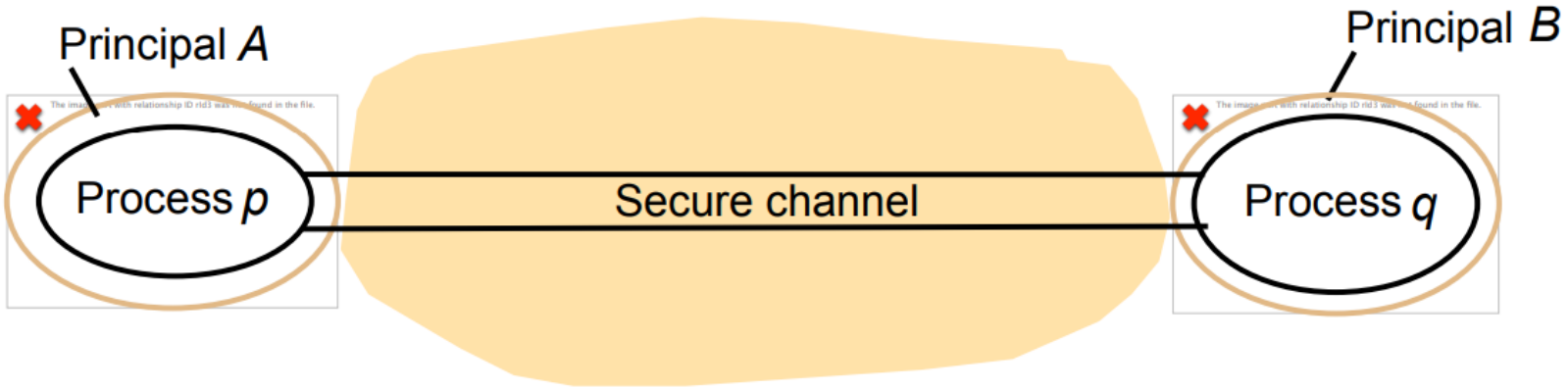
certificar conteúdos para garantir a sua autenticidade e não repúdio

Evitar/Esconder padrões regulares na comunicação entre Principais (por via de mensagens falsas/inúteis, aleatoriedade)

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Canais Seguros



Objectivo: trocar dados com **confidencialidade**, **integridade** e **autenticidade**

Num canal seguro os interlocutores (A e B) estão autenticados

O atacante **não pode** ler/copiar, alterar ou introduzir mensagens
O atacante **não pode** fazer replaying de mensagens (replaying = reenvio)
O atacante **não pode** reordenar as mensagens

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

- Canais Seguros
  - TLS Transport Layer Security (antigo Secure Socket Layer)
  - HTTPS - HTTP over TLS or HTTP Secure

Segurança em Sistemas Informáticos

Segurança em sistemas distribuídos

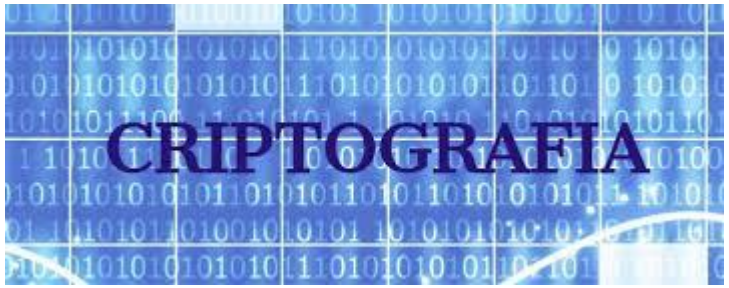
- Autenticação/Autorização: OAUTH
  - OAuth um protocolo standard e aberto para a autorização de acesso a recursos partilhados (tipicamente, na web)

  - Permite delegar a terceiros o acesso a recursos sensíveis, sem necessidade de lhes expor credenciais (passwords).

Exemplo:
Fotografias - recursos de um utilizador (o dono) armazenadas num servidor (base da confiança) podem ser acedidas por uma aplicação móvel (o cliente) ou por um serviço de impressão, sem que estes tenham acesso às credenciais geridas pelo servidor.

Segurança em sistemas distribuídos

- **Como Implementar**



Canais seguros

- Transmitir informação cifrada
- Autenticar parceiros de comunicação

Autorizar acesso restrito a dados

- Autenticar parceiros
- Criar e trocar testemunhos não forjáveis

Conceitos gerais sobre criptografia

- **Criptografia**

  - Para proteger as redes de comunicações, a criptografia é a ferramenta que permite evitar:
    - intercepção
    - manipulação
    - falsificação dos dados enviados

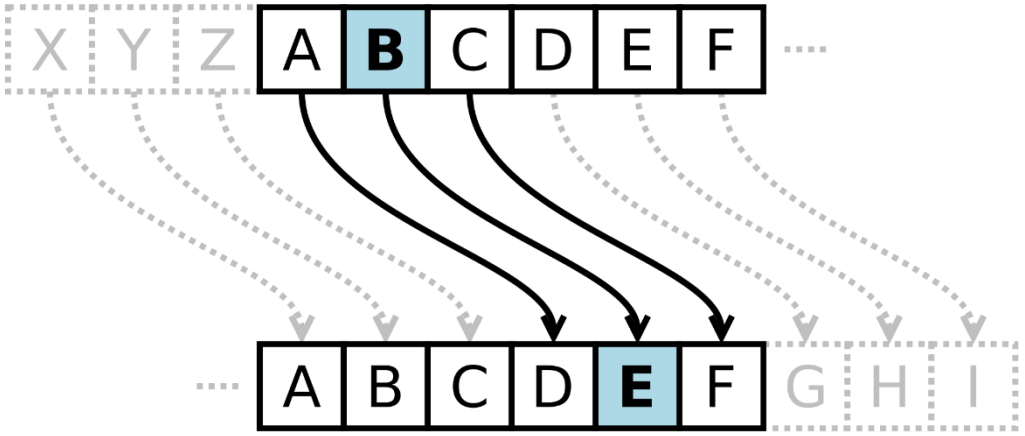
  - A finalidade básica da criptografia é o envio de informação secreta

Conceitos gerais sobre criptografia

- **Criptografia…ao longo da história.**
    - Ao longo da história têm sido concebidos diversos métodos para ocultar Informação
        - Antiga Grécia
        - Antigo Império Romano
            - atribui-se a Júlio César a criação de um método de cifra (designado por Cifra de César) para esconder informação dos inimigos

Segurança em Sistemas Informáticos

Conceitos gerais sobre criptografia



- **Na pré-história da criptografia**

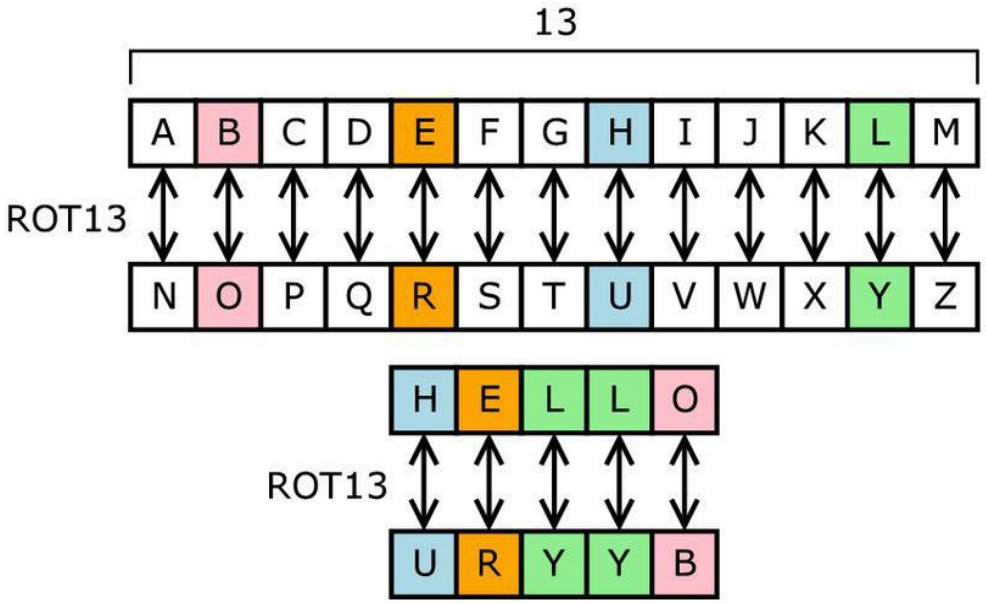
A ação de uma cifra de César é mover cada letra do alfabeto um número de vezes fixo abaixo no alfabeto. Este exemplo está com uma troca de três, então o B no texto normal se torna E no texto cifrado.

Chave = **3**

Conceitos gerais sobre criptografia

- **ROT13 – Evolução da cifra de César**

Cifra de substituição (“rotate by 13 places”)

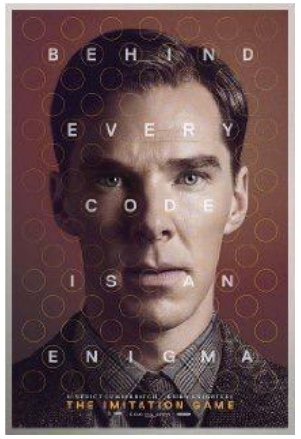


https://en.wikipedia.org/wiki/ROT13

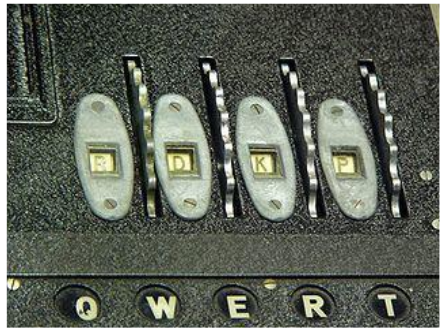
Segurança em Sistemas Informáticos

Conceitos gerais sobre criptografia

- **Criptografia ao longo da história**



WWII



https://www.youtube.com/watch?v=G2_Q9FoD-oQ

Conceitos gerais sobre criptografia

- **Chave**

- parâmetro que permite manipular as transformações aplicadas pela função criptográfica

- chave de cifra k, chave de decifra x
  - C = e(k, M)
  - M = d(x, C) = d(x, e(k, M))

Conceitos gerais sobre criptografia

- Um algoritmo criptográfico pode ser considerado como seguro se a um adversário for impossível obter um texto em claro M, conhecendo apenas
  - algoritmo de cifra
  - o texto cifrado C

- ou seja, é impossível decifrar a mensagem sem conhecer a chave

Segurança em Sistemas Informáticos

Conceitos gerais sobre criptografia

- Computacionalmente ou Incondicionalmente Seguro?
  - Segurança dos algoritmos de cifra
    - computacionalmente seguro
      - se aplicando o melhor método conhecido, a quantidade de recursos necessários (tempo de cálculo, número de processadores, etc.) para decifrar a mensagem sem conhecer a chave é muito maior da que está ao alcance de qualquer pessoa
    - incondicionalmente seguro
      - se não se puder inverter nem com recursos infinitos
  - Os algoritmos usados são habitualmente computacionalmente seguros

Conceitos gerais sobre criptografia

- Ataque: a acção de tentar decifrar mensagens sem conhecer a chave

- “quebrar” o algoritmo de cifra

    - cripto-análise: tentar analisar o algoritmo, ou os textos cifrados até conseguir encontrar algum com sentido

    - força-bruta: tentar todos os valores possíveis de uma chave de decifra, até se conseguir encontrar o correcto

Segurança em Sistemas Informáticos

Formas de ataques a mensagens cifradas – dependendo da informação disponível

Tipo de Ataque	Conhecido do Cripto-Analista
Apenas o texto cifrado	• Algoritmo de cifra • Texto cifrado a ser descodificado
Conhecido o texto em claro	• Algoritmo de cifra • Texto cifrado a ser descodificado • Um ou mais pares de texto em claro e texto cifrado formados com a chave secreta
Texto em claro escolhido	• Algoritmo de cifra • Texto cifrado a ser descodificado • Mensagem de texto em claro escolhida pelo cripto-analista, em conjunto com o texto cifrado gerado por uma chave secreta
Texto cifrado escolhido	• Algoritmo de cifra • Texto cifrado a ser descodificado • Texto cifrado escolhido pelo cripto-analista, em conjunto com o texto em claro gerado por uma chave secreta
Texto escolhido	• Algoritmo de cifra • Texto cifrado a ser descodificado • Mensagem de texto em claro escolhida pelo cripto-analista, em conjunto com o texto cifrado gerado por uma chave secreta • Texto cifrado escolhido pelo cripto-analista, em conjunto com o texto em claro gerado por uma chave secreta

Segurança em Sistemas Informáticos

Chave Simétrica

- Sistemas criptográficos de chave simétrica caracterizam-se por a chave de cifra ser igual à chave de decifra (ou que se pode deduzir directamente a partir desta)

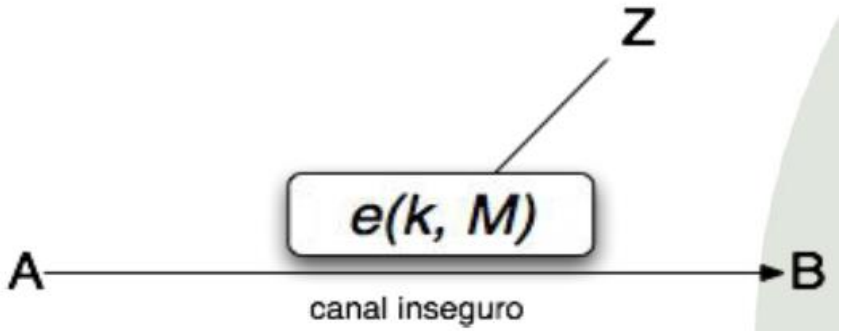
- Chave de cifra é igual à de decifra
  - x = k
  - C = e(k, M)
  - M = d(k, C) = d(k, e(K, M))

- A segurança deste sistema reside em manter em segredo a chave k

Segurança em Sistemas Informáticos

Chave Simétrica

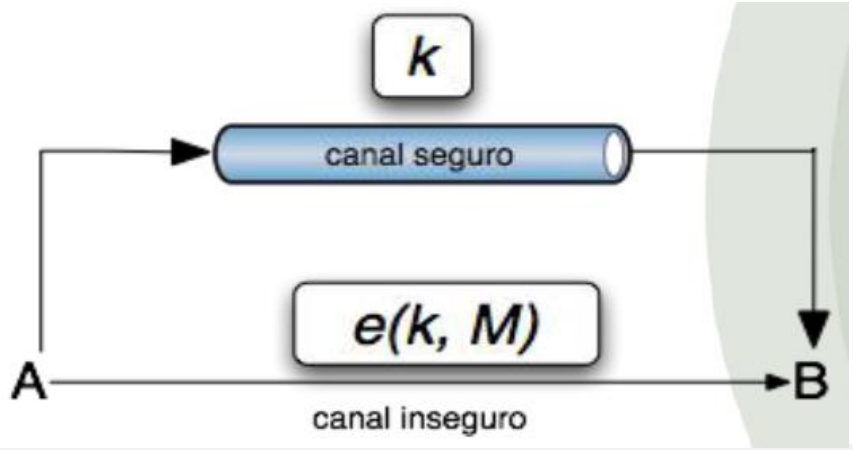
- Quando os participantes numa comunicação querem trocar mensagens confidenciais entre si, têm que escolher uma chave comum para trocar as mensagens



Segurança em Sistemas Informáticos

Chave Simétrica

- Se for usado um sistema deste tipo é necessário que a chave seja a mesma em A e em B
- Não se pode enviar a chave pelo mesmo canal pois o mesmo é inseguro
- Possível solução, usar um canal alternativo seguro

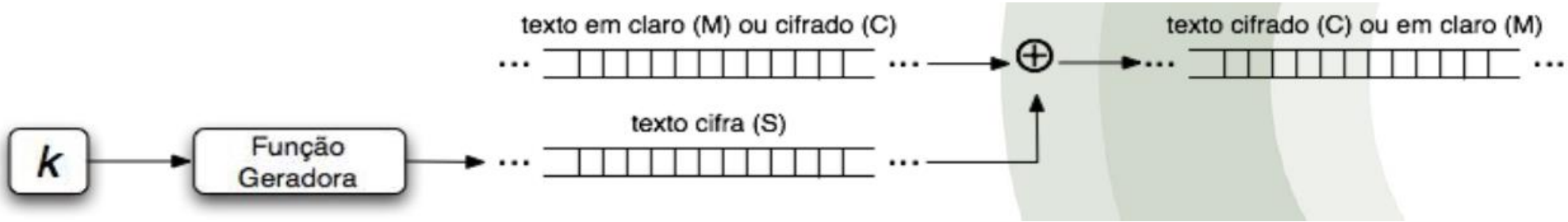


Segurança em Sistemas Informáticos

Chave Simétrica - Operações

- Se considerarmos o texto a cifrar formado por bits, a soma e subtração são equivalentes

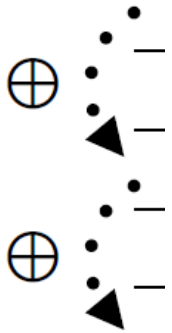
- Quando aplicadas bit a bit são iguais à operação lógica XOR (⊕) - (0⊕0=0, 0⊕1=1, 1⊕0=1, 1⊕1=0)
  - C = M⊕S(k)
  - M = C⊕S(k)



Segurança em Sistemas Informáticos

EXEMPLO

- Texto a cifrar: “PEDRO”
- Chave a usar: “XPTO12”
- ”PEDRO” em BIN: 01010000 01100101 01100100 01110010 01101111
- “XPTO12” em BIN: 01011000 01010000 01010100 01001111 00110001 00110010



P 01010000 01100101 01100100 01110010 01101111

K **01011000 01010000 01010100 01001111 00110001 00110010**

C 10110000 00000000 01100010 01010110 10000110 1011101

K **01011000 01010000 01010100 01001111 00110001 00110010**

P 01010000 01100101 01100100 01110010 01101111

P - Plaintext (texto em claro)
K - Key (Chave)
C - Ciphertext (texto cifrado)

Segurança em Sistemas Informáticos

Geração do texto de cifra

- Existem duas formas de obtenção do texto de cifra S em função de uma chave k
  - se se escolhe uma sequência k mais curta que a mensagem M, uma possibilidade seria repeti-la ciclicamente tantas vezes quanto necessário para a adicionar ao texto em claro
  - no outro extremo pode-se usar directamente S(k) = k. Isto quer dizer que própria chave deve ser tão grande como a própria mensagem
    - princípio conhecido como cifra de Vernam
    - se k for uma sequência totalmente aleatória estamos na presença de uma cifra incondicionalmente segura (one-time pad)

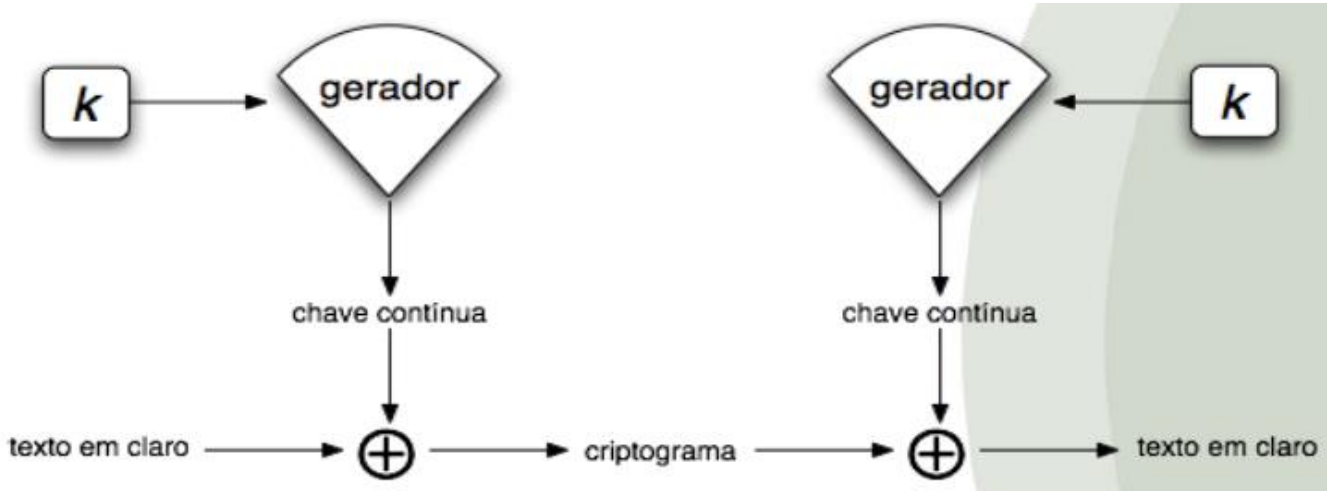
  - na prática, o que se usam são sequências pseudo-aleatórias geradas a partir de uma semente (seed, key-seed), e o que se partilha é unicamente esta semente

Segurança em Sistemas Informáticos

Gerador pseudo-aleatório seguro

- Comportamento do gerador é determinado por uma chave de dimensão fixa k

- A chave contínua produzida é depois misturada com o texto original de forma invertível (mod 2, XOR)



Segurança em Sistemas Informáticos

Cálculo Modular (101)

- Pensar num relógio
- 13 mod 12 = 1
- 12 seria o número de divisões do relógio
- 13 o número de passagens por essas divisões
- Resto da divisão entre de 13 por 12 = 1

- 50 mod 12 = 2
- 50 mod 50 = 0
- ...

Segurança em Sistemas Informáticos

Cifra de Vernam - Exemplo

- Mensagem a cifrar: “LOCAL DA REUNIAO SECRETA NA ATEC”
- Retiramos os espaços: “LOCALDAREUNIAOSECRETANATEC”
- Usamos uma chave com a mesma dimensão do texto a cifrar: “XBFGDERTQWERTYUIOPAQRTUVLPOI”
- Usamos uma tabela para facilitar o cálculo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Para cifrar: Pi + Ki mod 26
- Por exemplo, L + X mod 26 = 12 + 24 mod 26 = 36 mod 26 = 10 = J

Segurança em Sistemas Informáticos

Cifra de Vernam - Exemplo

- Mensagem a cifrar: “LOCAL DA REUNIAO SECRETA NA ATEC”
- Retiramos os espaços: “LOCALDAREUNIAOSECRETANATEC”
- Usamos uma chave com a mesma dimensão do texto a cifrar: “XBFGDERTQWERTYUIOPAQRTUVLPOI”
- Usamos uma tabela para facilitar o cálculo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

- Para cifrar: Pi + Ki mod 26
- Por exemplo, L + X mod 26 = 12 + 24 mod 26 = 36 mod 26 = 10 = J

Segurança em Sistemas Informáticos

Cifra de Vernam – Exemplo - Decifrar

- Decifra –> Ci - Ki mod 26
  - J - X mod 26 = 10 - 24 mod 26 = -14 mod 26 = 12 = L

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

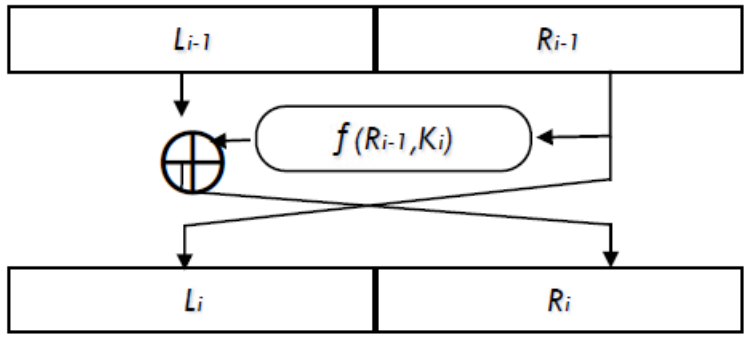
P - Plaintext (texto em claro)
K - Key (Chave)
C - Ciphertext (texto cifrado)

Segurança em Sistemas Informáticos

Rede de Feistel

- Operação complexa mais utilizada para efectuar diversas iterações

- Transforma um bloco, constituído por dois sub-blocos de comprimento igual L_{i-1} e R_{i-1}, num outro bloco de igual dimensão, formado pelos blocos L_i e R_i, de acordo com:



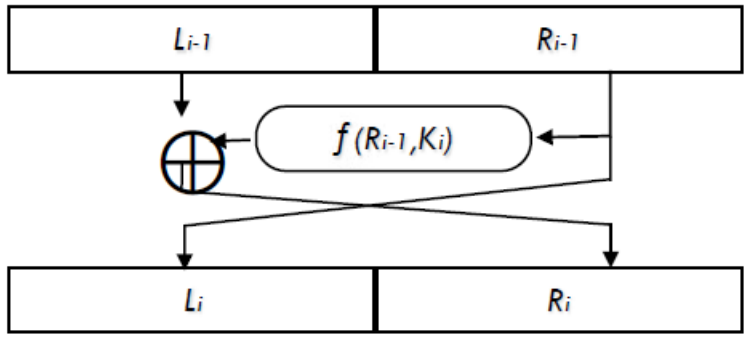
$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

f é uma função complexa, não-linear, que produz um valor dado um sub-bloco e uma sub-chave K_i derivada da chave global ***K***.

Segurança em Sistemas Informáticos

Rede de Feistel

- Permite fazer a decifra tão facilmente como se faz a cifra
- Inverte-se apenas o sentido de cálculo



$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$$

f é uma função complexa, não-linear, que produz um valor dado um sub-bloco e uma sub-chave K_i derivada da chave global ***K***.

Segurança em Sistemas Informáticos

Rede de Feistel

- Alguns algoritmos que usam redes de Feistel
  - DES
  - Lucifer
  - FEAL
  - Khufu
  - Khafre
  - LOKI
  - GOST
  - CAST
  - Blowfish

Segurança em Sistemas Informáticos

Comparação entre alguns algoritmos de cifra de bloco

	Bloco (bits)	Chave (bits)	Iterações Internas
DES	64	56	16
CAST	64	64	8
IDEA	64	128	8
Blowfish	64	Variável até 448	16
AES (Rijndael)	128,192 ou 256	128, 192 ou 256	10, 12 ou 14
RC5	variável	variável	variável

Segurança em Sistemas Informáticos

Algoritmo de Cifra de Bloco – DES (Data Encryption Standard)

- Na década de 1970 surge a necessidade de uma cifra robusta para ambientes comerciais (na altura as cifras existiam essencialmente em ambientes militares)

- Em 1973 o National Bureau of Standards (NBS) abre um concurso para selecção da cifra

- Requisitos:
  - elevado nível de segurança
  - algoritmo completamente especificado e fácil de perceber
  - algoritmo público, sendo a segurança fornecida pelo secretismo das chaves
  - capacidade para ser usado em diversos cenários operacionais, capacidade para operar em dados de qualquer tipo
  - economicamente realizável, em dispositivos electrónicos dedicados
  - eficiente
  - susceptível de validação
  - susceptível de exportação

Segurança em Sistemas Informáticos

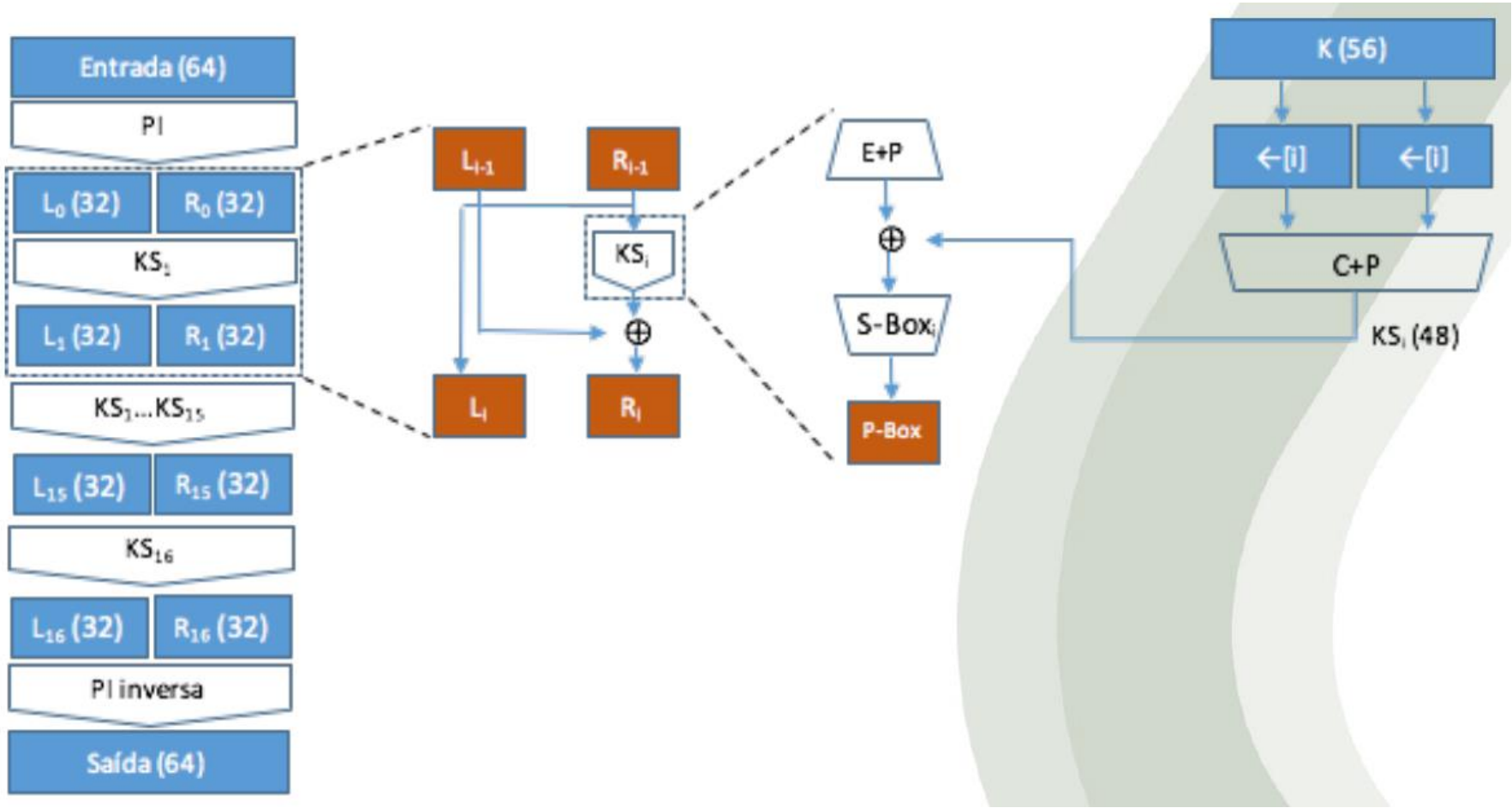
Algoritmo de Cifra de Bloco – DES (Data Encryption Standard)

- Foi escolhido o algoritmo apresentado pela IBM, Lucifer
- Foi adoptado como padrão em 1977

- Cifra simétrica por blocos, usando blocos de 64 bits e chaves de 56 bits
- Diversos modos de operação: ECB, CBC, OFB e CFB
- 16 iterações com redes de Feistel

Segurança em Sistemas Informáticos

Modo de operação do DES (Data Encryption Standard)



Segurança em Sistemas Informáticos

Modos de Cifra de Bloco: ECB, CDB, CBF, OFB, CTR

- O modo de cifra estabelece o modelo de aplicação de um algoritmo de cifra a um texto de dimensão arbitrária
- Existem dois tipos genéricos radicalmente diferentes de modos de cifra
    - Um dos tipos efectua o pré-processamento dos dados a cifrar antes dos mesmos serem cifrados pelo algoritmo de cifra, e pós-processamento do resultado fornecido pelo último
        - ECB, CBC
        - usados no DES, AES
- O outro tipo consiste em usar um algoritmo de cifra de blocos para realizar cifra contínua, em que o algoritmo de cifra por blocos é usado para calcular o estado seguinte da máquina de estados do gerador da chave contínua
        - OFB, CFB, CTR
        - usado no DES, AES

ECB – Electronic Code Book

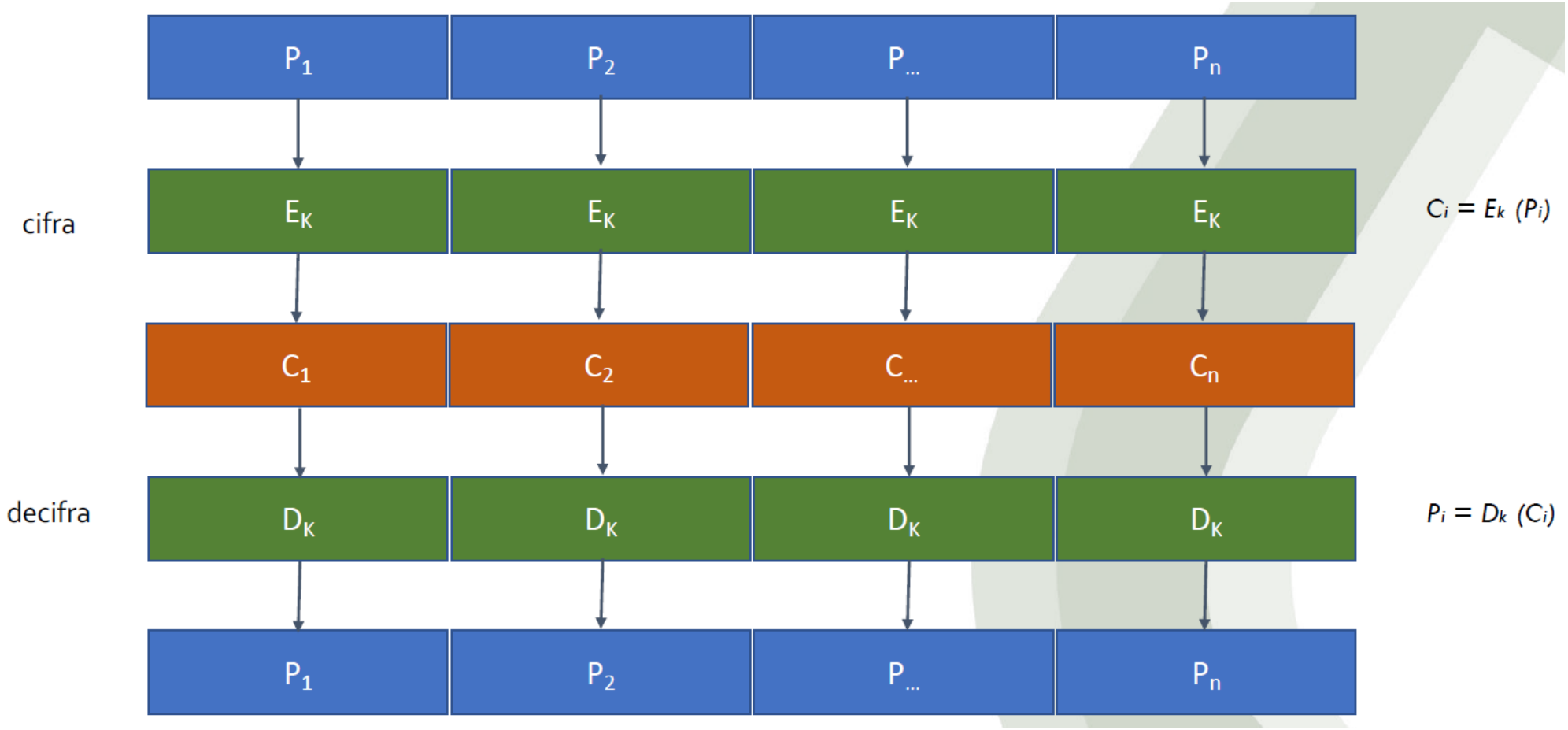
- Método mais simples e intuitivo de usar uma cifra por blocos
- Consiste em dividir o texto em blocos independentes e contíguos que são cifrados independentemente

$$\forall_{i,j}\ ,\ i \neq j,\ P_i = P_j \Rightarrow C_i = C_j$$

- Uma das fraquezas do ECB é a reprodução de padrões de texto original, porque dois blocos iguais de texto original produzem dois blocos iguais no criptograma

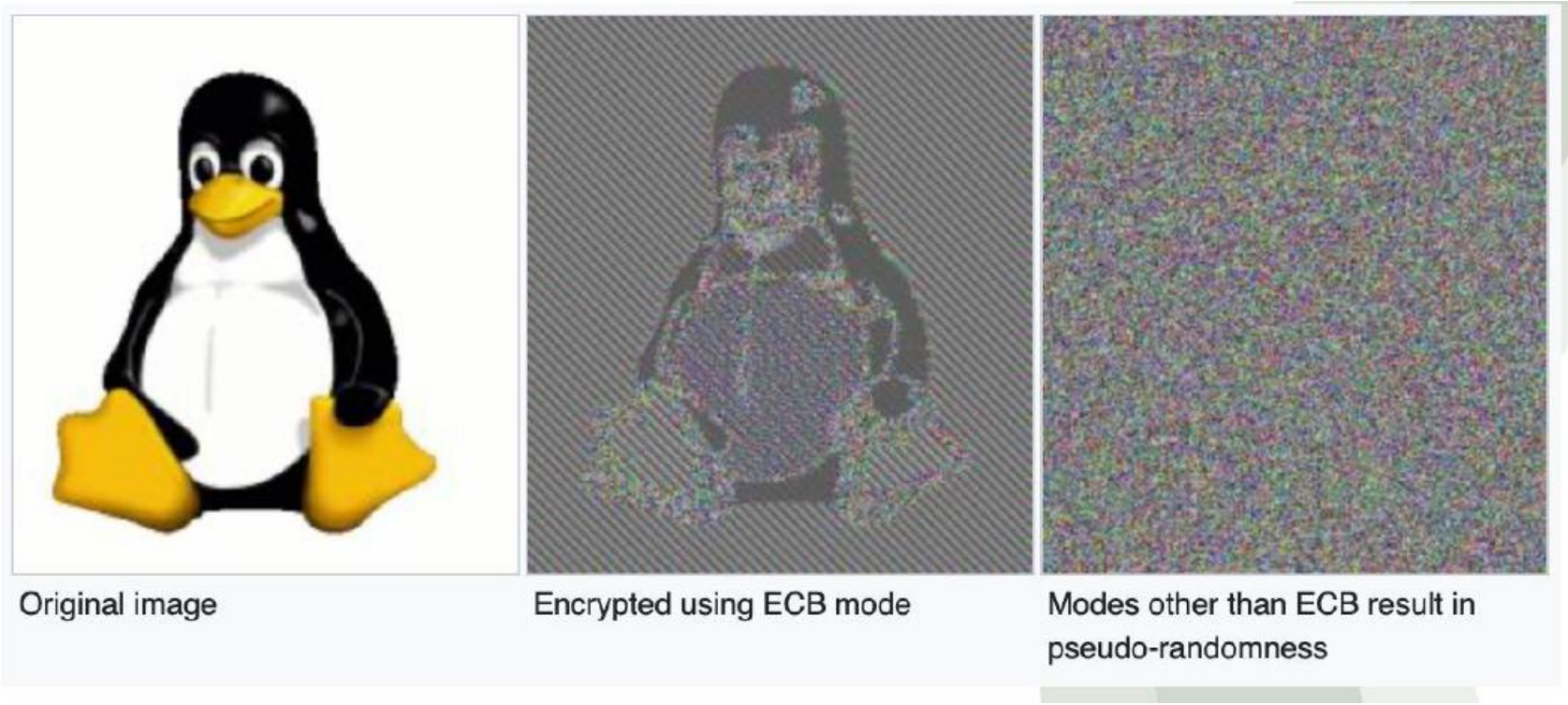
Segurança em Sistemas Informáticos

ECB – Electronic Code Book



Segurança em Sistemas Informáticos

ECB – Electronic Code Book



Original image

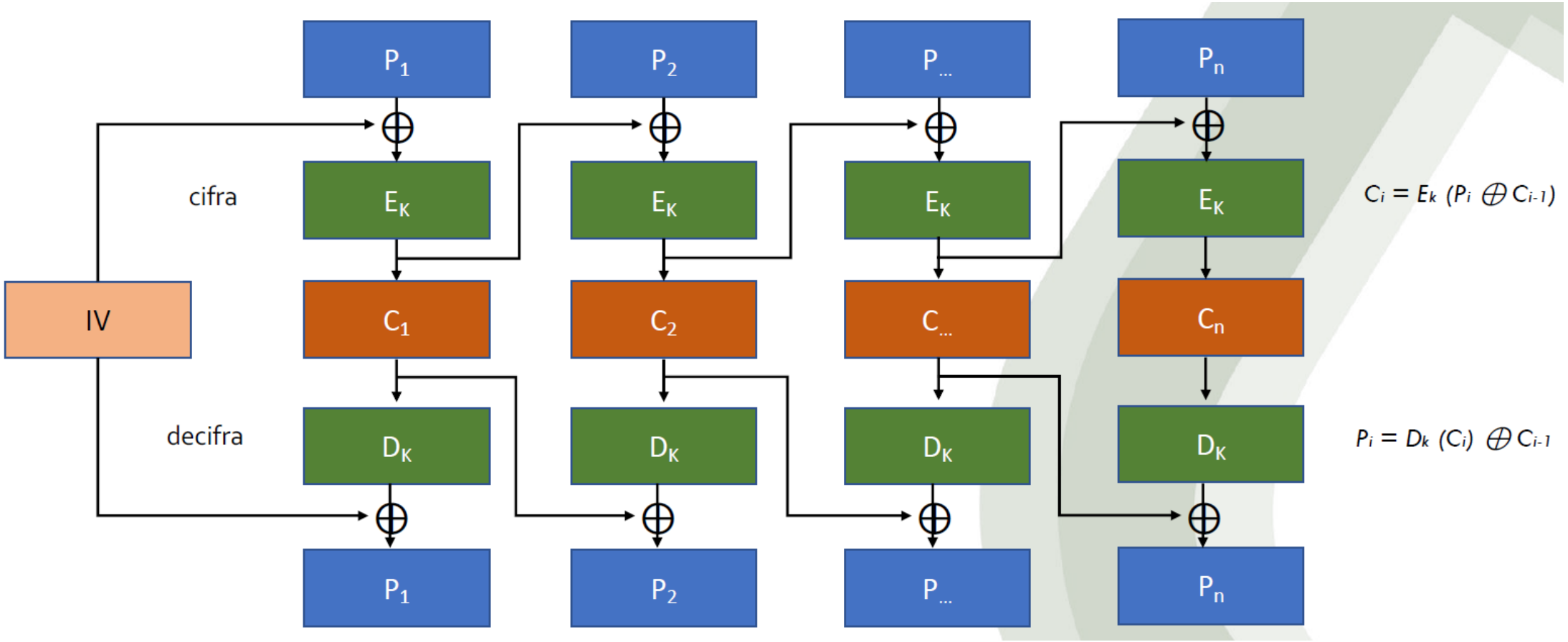
Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Segurança em Sistemas Informáticos

CBC – Cipher Block Chaining

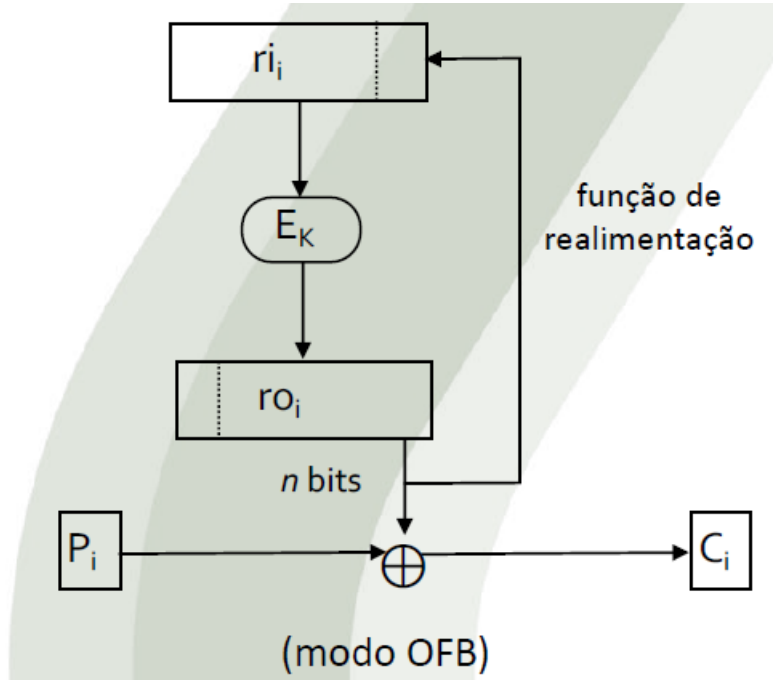


Segurança em Sistemas Informáticos

OFB, CFB e CTR

- OFB = Output Feedback
- CFB = Cipher Feedback
- CTR = Counter
- Transformam uma cifra de blocos em cifra continua
- Nestes modos, não existe necessidade de **padding**

- Método base:
  - O gerador de cifra contínua é constituído por
    - Uma função de cifra por blocos
    - Dois registos com o comprimento do bloco, ri e ro
    - Função de realimentação



P_i e C_i = i-ésimo bloco de n bits de um texto e de um criptograma
E_K = uma função de cifra por blocos com base na chave K
ri_i e ro_i = valor dos registos ri e ro na i-ésima iteração

Segurança em Sistemas Informáticos

Algoritmo de Cifra de Bloco – AES (Advanced Encryption Standard)

- **KeyExpansion** - chaves da iteração são derivadas a partir da chave de cifra usando a tabela de expansão de chaves do Rijndael
- Iteração inicial
  - **AddRoundKey** - cada byte da matriz de estado é combinado com a chave de iteração usando XOR bit-a-bit
- Iterações
  - **SubBytes** - passo de substituição não-linear em que cada byte é substituído por outro de acordo com uma tabela de pesquisa
  - **ShiftRows** - um passo de transposição em que cada linha da matriz de estado é shiftada ciclicamente um determinado número de vezes
  - **MixColumns** - uma operação de mistura que opera nas colunas da matriz de estado, combinando os quatro bytes em cada coluna
  - **AddRoundKey**
- Iteração Final (sem MixColumns)
  - **SubBytes**
  - **ShiftRows**
  - **AddRoundKey**

https://www.youtube.com/watch?v=mlzxpkdXP58

Segurança em Sistemas Informáticos

Funções de Síntese/Resumo

- **Não servem para cifrar e decifrar dados**

- **Servem para complementar, com segurança criptográfica, outros mecanismos de segurança**
  - **úteis para gerar e validar assinaturas digitais**
  - **para calcular autenticadores de mensagens**
  - **para derivar chaves a partir de chaves mestre ou senhas textuais**

- **Produzem valores de dimensão constante a partir de textos de dimensão variável**

- **Funcionam com base em funções de compressão**

Segurança em Sistemas Informáticos

Funções de Síntese/Resumo

- **Não servem para cifrar e decifrar dados**

- **Servem para complementar, com segurança criptográfica, outros mecanismos de segurança**
  - **úteis para gerar e validar assinaturas digitais**
  - **para calcular autenticadores de mensagens**
  - **para derivar chaves a partir de chaves mestre ou senhas textuais**

- **Produzem valores de dimensão constante a partir de textos de dimensão variável**

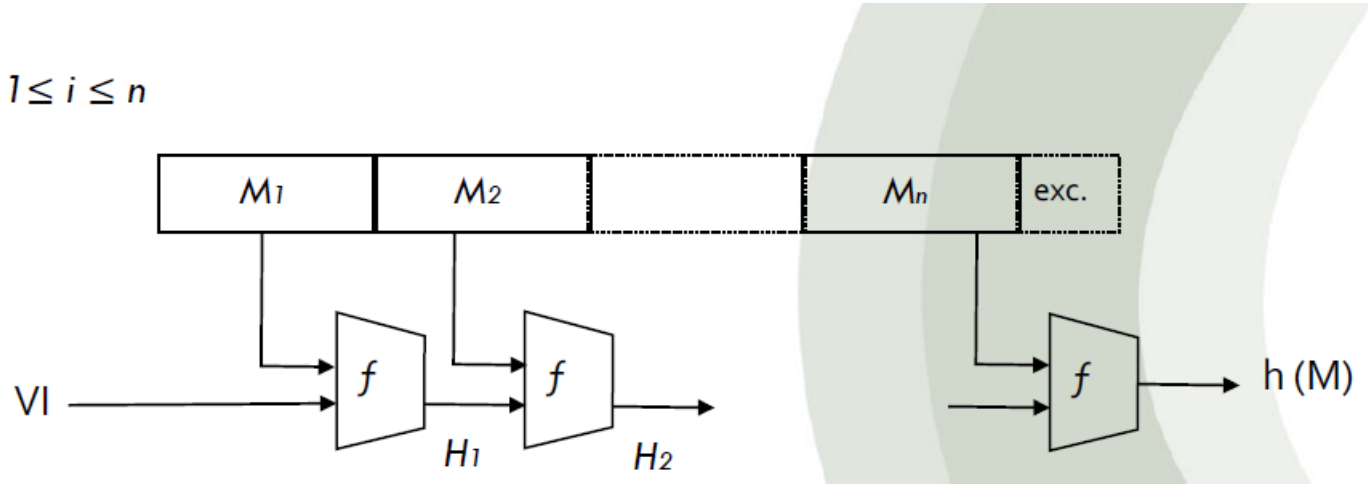
- **Funcionam com base em funções de compressão**

Segurança em Sistemas Informáticos

Funções de Síntese/Resumo

- **Dados dois valores, um com uma síntese prévia e outro com o valor a processar, produz uma nova síntese**

$$\begin{cases} H_0 = VI \\ H_i = f(H_{i-1}, M_i),\ 1 \le i \le n \\ h(M) = H_n \end{cases}$$



Segurança em Sistemas Informáticos

Funções de Síntese/Resumo – Alguns dos algoritmos mais usados

- **Funções síntese/resumo (digest functions)**
  - **MD5 (128) (obsoleto)**
  - **SHA-1(160) (obsoleto)**
  - **RIPEMD-128/160**
  - **SHA-2 (SHA-256, SHA-512, …)**
  - **SHA-3 (Keccak) (SHA3-512, SHAKE256,…)**
  - **Whirlpool (512)**

Segurança em Sistemas Informáticos

Autenticadores de Dados e Mensagens

- Conjuntos de bits que acompanham mensagens e que **garantem a sua correcção e origem**
  - Os valores gerados apenas a partir das mensagens por funções de síntese, não são suficientes para este fim - apenas garantem correcção e não a origem

- Para garantir a **origem,** os autenticadores de dados têm que incluir na sua geração e validação **dados secretos** ou **cifras**

- Consoante o tipo de chaves usadas (**simétricas** ou **assimétricas**), podemos ter:
  - autenticadores de mensagens
  - assinaturas digitais

Segurança em Sistemas Informáticos

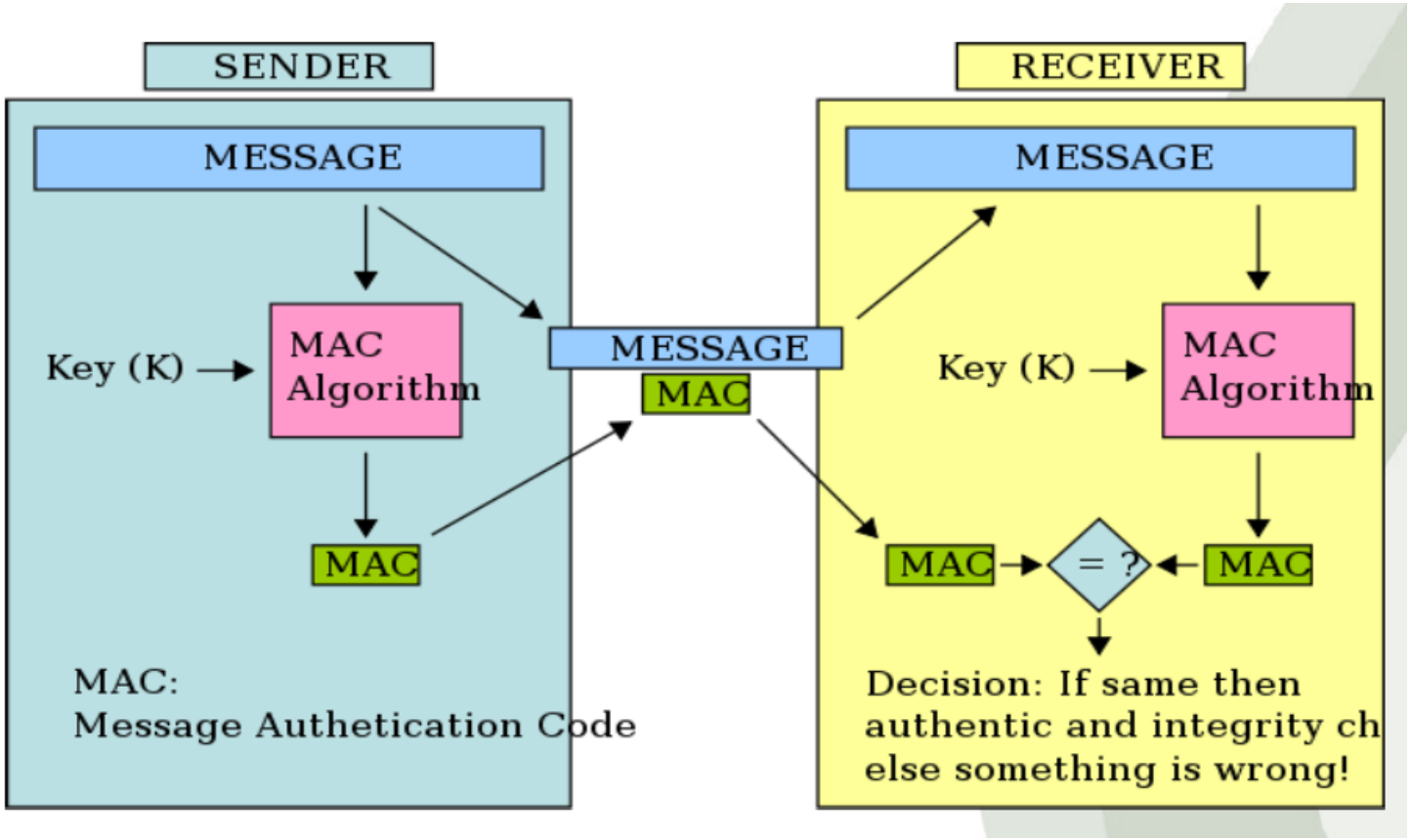
Autenticadores de Dados e Mensagens

- **Autenticadores de mensagens**
  - Message Authentication Code - MAC
  - Valor produzido a partir de uma **mensagem** e de uma **chave simétrica** partilhada pelo emissor e receptor
  - MAC pode apenas ser gerado e validado pelas entidades que partilham a mesma chave secreta
  - Prova que um dos interlocutores produziu a mensagem que contém o MAC (a não ser que a chave secreta tenha sido comprometida)
- Formas de produção do MAC
  - cifrar a mensagem e o seu resumo com cifra de blocos
  - usar funções com chaves, baseadas em
    - funções de cifra por blocos
    - funções de cifra contínua
    - funções de síntese/resumo

Segurança em Sistemas Informáticos

Autenticadores de Dados e Mensagens

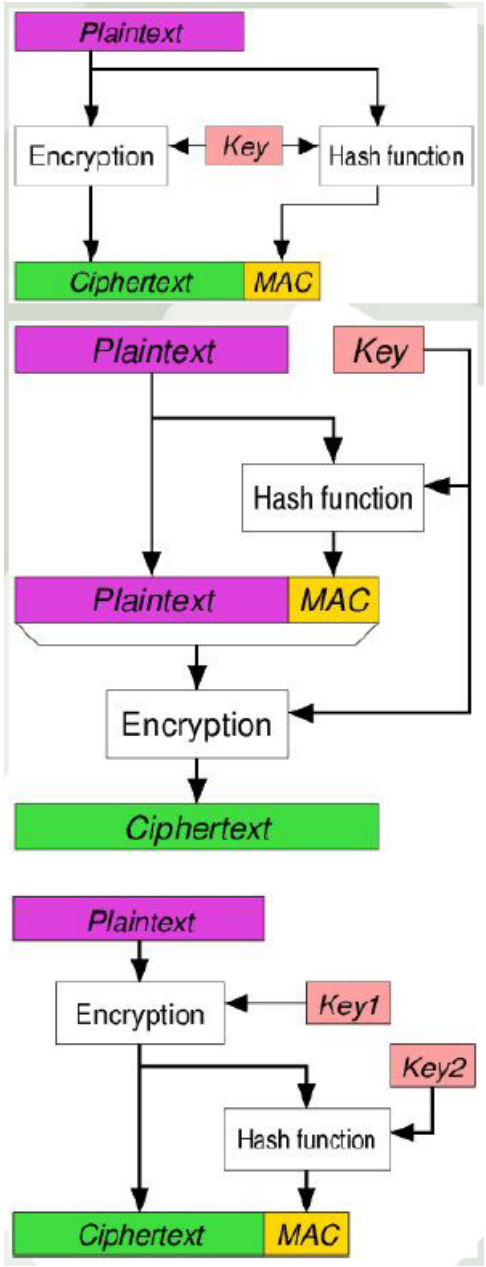
- **Autenticadores de mensagens**



Segurança em Sistemas Informáticos

Autenticadores de Dados e Mensagens

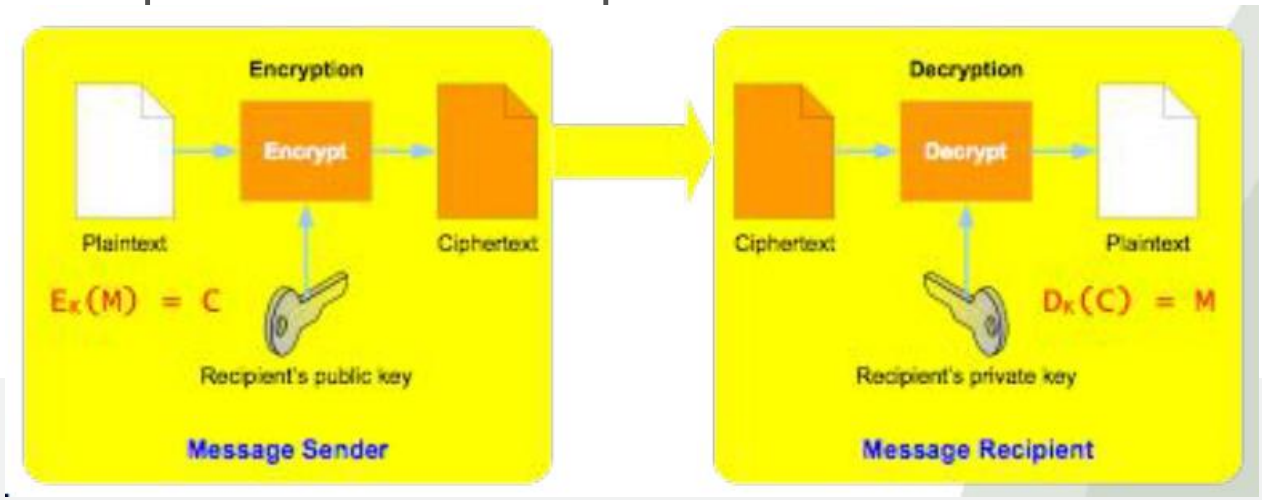
- **Autenticadores de mensagens**
- Quando se usa um MAC para autenticar uma mensagem cifrada (cifra autenticada), há várias formas de enquadrar a cifra da mensagem e a produção de um MAC da mesma:
  - Produzir o MAC a partir da mensagem em claro, e enviá-lo em claro em conjunto com a mensagem cifrada (**Encrypt-and-MAC**): SSH
  - Produzir MAC a partir da mensagem em claro e cifrá-lo em conjunto com a mensagem (**MAC-then-Encrypt**): SSL
  - Cifrar a mensagem e produzir um MAC, a partir do criptograma resultante (**Encrypt-then-MAC**): IPsec



Segurança em Sistemas Informáticos

Criptografia de Chave-Pública

- Ajuda a resolver o problema da distribuição das chaves secretas
- Usa um par de chaves
  - pública
  - privada
- As chaves pública (Kpub) e privada (Kpriv) têm uma relação matemática entre si
- A chave pública é derivada da chave privada
  - apenas o dono tem a chave privada
  - a chave privada não pode ser deduzida (em teoria) através da análise da chave pública
- O que é cifrado com uma das chaves só pode ser decifrado pela outra
- Exemplos:
  - Diffie-Helman
  - RSA
  - ElGamal



Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – Problemas Matemáticos Complexos

- Criptografia assimétrica é matematicamente mais complexa que a criptografia simétrica
  - Algoritmos de **Factorização**
  - Algoritmos de **Logaritmos Discretos**
    - Logaritmos discretos em **Campos Finitos**
    - Logaritmos discretos de **Curvas Elípticas em Campos Finitos**
- O processo de criptografia de chave pública é substancialmente mais lento que os processos de criptografia de chave simétrica (100 vezes mais lento em software, entre 1000 a 10000 vezes mais lento em hardware)
- A dimensão das chaves devem ser consideravelmente grandes (1024 bits ou mais)

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – RSA

- Inventado em 1977
- **R**ivest, **S**hamir e **A**dleman
- Baseia a sua segurança na **complexidade de factorização e cálculo de logaritmos modulares** (de grandes números - 512, 1024, 2048, ... bits)

- Usa-se para **cifrar** e **decifrar** informação
- Usa-se para **assinar digitalmente** e **verificar a assinatura** de informação

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – RSA

Valores Públicos	n	Valor de grande dimensão (centenas de bits), produto de dois grandes primos p e q secretos: $n = p.q$
Chave pública	e	$e < n$, co-primo de $\Phi(n) = (p-1)(q-1)$
Chave privada	p, q, d	$d < n$, $e.d \equiv 1 \pmod{\Phi(n)}$
Cifra	$C = P^e \bmod n$	
Decifra	$P = C^d \bmod n$	

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – Cálculo do RSA

- Cálculo do par de Chaves
- Escolher dois números primos grandes, **p** e **q** (secretos)
- Calcular **n=pq**, e **Φ(n)=(p-1)(q-1)**
- Encontrar um número e que seja primo relativo de **Φ(n)**
- Chave pública: **e** e **n**
- Encontrar um número **d** que seja o inverso multiplicativo de **e mod Φ(n)**
- Chave privada: **d** e **n**

- **Cifra**
  - **Calcular: $c = m^e \bmod n$**
- **Decifra**
  - **Calcular: $m = c^d \bmod n$**

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – Cálculo do RSA (Exemplo prático)

- RSA (exemplo prático):
- escolher dois números primos
  - p = 61 e q = 53
- calcular n = pq
  - n = 61.53 = 3233
- calcular Φ(n) = (p-1) (q-1)
  - Φ(n) = (61-1)(53-1) = 3120
- encontrar e que seja primo relativo de Φ(n) – encontra um valor que não seja divisor de Φ(n)
  - e = 17
- encontrar o d que seja o inverso multiplicativo de e mod Φ(n)
  - $d \equiv 17 \bmod 3120$
  - $d.17 \equiv 1 \bmod 3120$
  - d = 2753
  - uma vez que 2753.17 = 46801 e 46801 mod 3120 = 1, portanto o complicado é encontrar um número d, cuja multiplicação com e, e dividido por Φ(n), o resto da divisão seja 1
- chave pública
  - n = 3233, e = 17
- chave privada
  - n = 3233, d = 2753

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – Cálculo do RSA (Exemplo prático)

- RSA (exemplo prático):
- chave pública
  - n = 3233, e = 17
- chave privada
  - n = 3233, d = 2753
- cifrar informação
  - c = m17 mod 3233
  - cifrar 123, c = 12317 mod 3233, c = 855
- decifrar informação
  - m = c2753 mod 3233
  - decifrar 855, m = 8552753 mod 3233, m = 123

Segurança em Sistemas Informáticos

Criptografia de Chave-Pública

- Logaritmos discretos em Campos Finitos
- Baseados na prova matemática do problema generalizado dos logaritmos discretos
  - em que calcular exponenciação sobre um campo finito é simples ($Y^x \bmod P$)
  - mas calcular o logaritmo discreto é difícil (encontrar x em que $Y^x \equiv Z \pmod P$)
- Parâmetros têm que ser igualmente grandes como no caso da factorização (512, 1024, 2048-bit).
- Exemplos: Diffie-Hellman, El Gamal, e DSA.
- Ataques de força bruta não funcionam contra estes. Mas podem ser vulneráveis a ataques de textos cifrados escolhidos (chosen-ciphertext attacks).

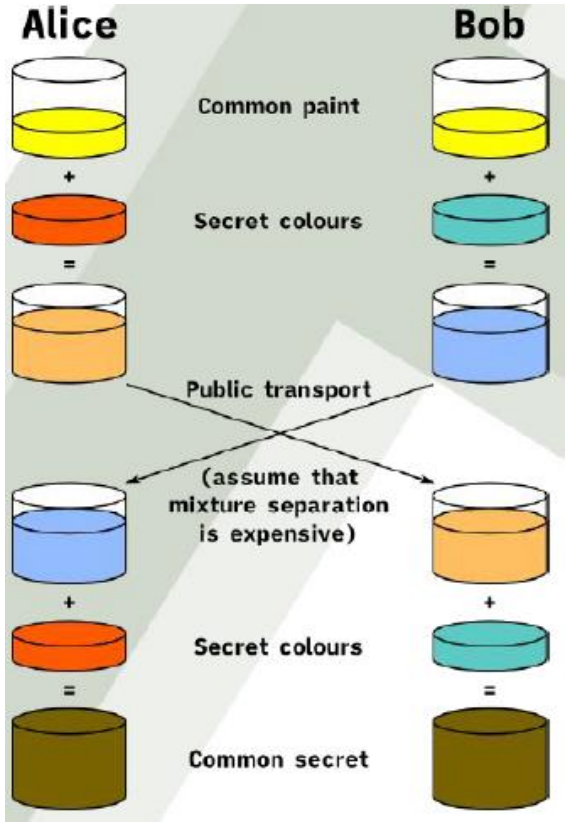
Segurança em Sistemas Informáticos

Criptografia de Chave-Pública – Key-agreement protocolo

- Diffie-Hellman
- Primeiro algoritmo de Chave Pública
- Inventado em 1976 por Diffiel e Hellman
- É essencialmente um keyagreement-protocol

Alice				Bob		
Secreto	Público	Calcula	Envia	Calcula	Público	Secreto
a	p, g		p,g→			b
a	p, g, A	$g^a \bmod p = A$	A→		p, g	b
a	p, g, A		← B	$g^b \bmod p = B$	p, g, A, B	b
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

- Funcionamento:

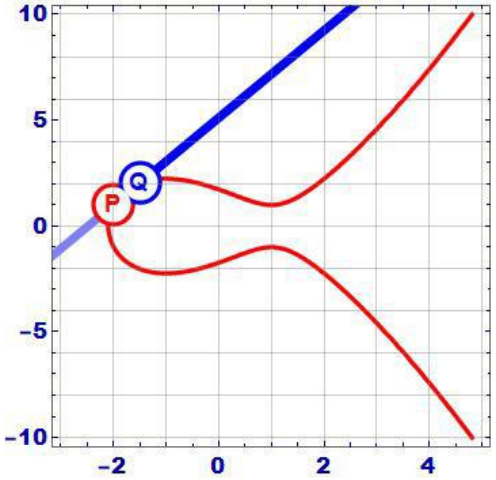


Segurança em Sistemas Informáticos

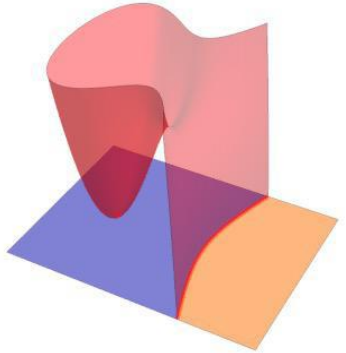
Criptografia de Chave-Pública – Mais eficiente

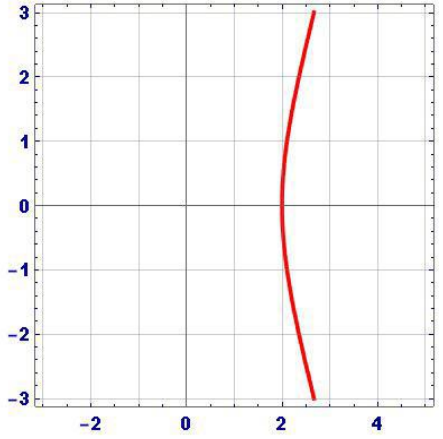
$$ay^2 + by = cx^3 + dx^2 + ex + f \quad \{a, b, c, d, e, f\} \in \mathbb{R}$$

The general form of the elliptic curve equation



- A Criptografia de Curva Elíptica (Elliptic Curve Cryptography (ECC)) usa um sistema algébrico definido em pontos de uma curva elíptica para oferecer criptografia de chave pública
  - Baseia-se no problema matemático de factores que são pares de coordenadas que fazem parte de uma determinada curva elíptica
  - Problema: encontrar um logaritmo discreto de uma curva elíptica aleatória respeitante a um ponto-base público, é impossível.
- Vantagens:
  - Oferece a maior robustez por bit dos sistemas de criptografia de chave publica.
  - Maiores velocidades na cifra e assinatura.
  - Menores assinaturas e certificados (ideais para smartcards).
- Exemplos:
  - ECC, EC-DH, EC-DSA, EC-ElGamal





Segurança em Sistemas Informáticos

Criptografia de Chave-Pública

	Encryption	Digital Signature	Hash Function	Key Distribution
Symmetric Key Algorithms				
DES	X			
3DES	X			
AES	X			
Blowfish	X			
IDEA	X			
RC4	X			
Asymmetric Key Algorithms				
RSA	X	X		X
ECC	X	X		X
ElGamal, EC-ElGamal	X	X		X
DSA, EC-DSA		X		
Diffie-Hellman (DH), EC-DH				X
Hash Function				
RSA: MD2, MD4, MD5			X	
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512			X	
HAVAL			X	

Segurança em Sistemas Informáticos

Gestão de Chaves

- Conjunto de **técnicas** e de **procedimentos** que suportam o estabelecimento e manutenção de relações baseadas em chaves entre partes autorizadas.

- A Gestão de Chaves **suporta técnicas e procedimentos** para:
  - A inicialização de utilizadores e de sistemas dentro de um determinado domínio;
  - Geração, Distribuição e instalação de chaves;
  - Controlar a utilização de chaves;
  - Actualização, revogação e destruição de chaves;
  - Armazenamento, backup/recuperação e arquivo de chaves.

Segurança em Sistemas Informáticos

Gestão de Chaves

- O **objectivo** da Gestão de Chaves é a de **manter as relações entre chaves e as próprias chaves de uma forma que contrarie ameaças relevantes,** tais como:
  - Compromisso das chaves secretas;
  - Compromisso da autenticidade de chaves secretas ou públicas;
  - Uso não-autorizado de chaves secretas ou públicas.

Segurança em Sistemas Informáticos

Gestão de Chaves

- A Gestão de Chaves é oferecida no contexto de uma política de segurança
- A política de segurança implícita ou explicitamente define as ameaças que um sistema poderá enfrentar
- A **política de segurança** especifica:
  - As práticas e os procedimentos que devem ser seguidos na execução dos aspectos técnicos e administrativos da Gestão de Chaves, tanto automáticos como manuais;
  - As responsabilidades de cada uma das partes envolvidas;
  - Os tipos de registos a serem mantidos, para suportar relatórios posteriores ou revisão de eventos relacionados com segurança.

Segurança em Sistemas Informáticos

Gestão de Chaves – Cripto-Período

- O cripto-período de uma chave é o intervalo de tempo durante o qual uma chave é válida para utilização pelas partes legítimas

- Serve para:
  - Limitar a informação de uma chave para cripto-analistas;
  - Limitar a exposição de uma chave no caso de compromisso da mesma;
  - Limitar a utilização de uma tecnologia particular ao seu tempo de vida estimado;
  - Limitar a disponibilidade de tempo que existe para serem efectuados ataques de criptanálise computacionalmente intensivos.

Segurança em Sistemas Informáticos

Gestão de Chaves – Cripto-Período

Chaves a longo prazo

Incluem-se nesta categoria chaves-mestre, chaves de cifra de outras chaves, e chaves utilizadas para o estabelecimento de outras chaves

Chaves a curto prazo

Incluem-se chaves estabelecidas por protocolos de key agreement, chaves de sessão ou de cifra temporária.

Segurança em Sistemas Informáticos

Gestão de Chaves – Cripto-Período

NIST SP 800-57, Recommendation on Key Management

Key Type	Crypto-period	
	Originator Usage Period	Recipient Usage Period
1. Private Signature Key	1-3 years	
2. Public Signature Key	Several years (depends on key size)	
3. Symmetric Authentication Key	≤ 2 years	≤ OUP + 3 years
4. Private Authentication Key	1-2 years	
5. Public Authentication Key	1-2 years	
6. Symmetric Data Encryption Keys	≤ 2 years	≤ OUP + 3 years
7. Symmetric Key Wrapping Key	≤ 2 years	≤ OUP + 3 years
8. Symmetric and asymmetric RNG Keys	Upon reseeding	
9. Symmetric Master Key	About 1 year	
10. Private Key Transport Key	≤ 2 years	

Segurança em Sistemas Informáticos

Gestão de Chaves – Cripto-Período

NIST SP 800-57, Recommendation on Key Management

Key Type	Crypto-period	
	Originator Usage Period	Recipient Usage Period
11. Public key Transport Key	1-2 years	
12. Symmetric Key Agreement Key	1-2 years	
13. Private Static key Agreement Key	1-2 years	
14. Public Static Key Agreement Key	1-2 years	
15. Private Ephemeral Key Agreement Key	One key agreement transaction	
16. Public Ephemeral Key Agreement Key	One key agreement transaction	
17. Symmetric Authorization Key	≤ 2 years	
18. Private Authorization Key	≤ 2 years	
19. Public Authorization Key	≤ 2 years	

Segurança em Sistemas Informáticos

Gestão de Chaves – Ciclo de vida das chaves

- A sequência de estados que uma chave atravessa ao longo do seu tempo de vida designa-se por Gestão do Ciclo de Vida de uma Chave.
- Estados dentro do ciclo de vida:
  - Pré-operacional
    - A chave ainda não está disponível para operações criptográficas
  - Operacional
    - A chave está disponível para utilização normal
  - Pós-operacional
    - A chave já não é utilizada, mas acesso offline à mesma é ainda possível para efeitos específicos
  - Obsoleta
    - A chave já não está disponível. Todos os registos que envolvam a chave são apagados.

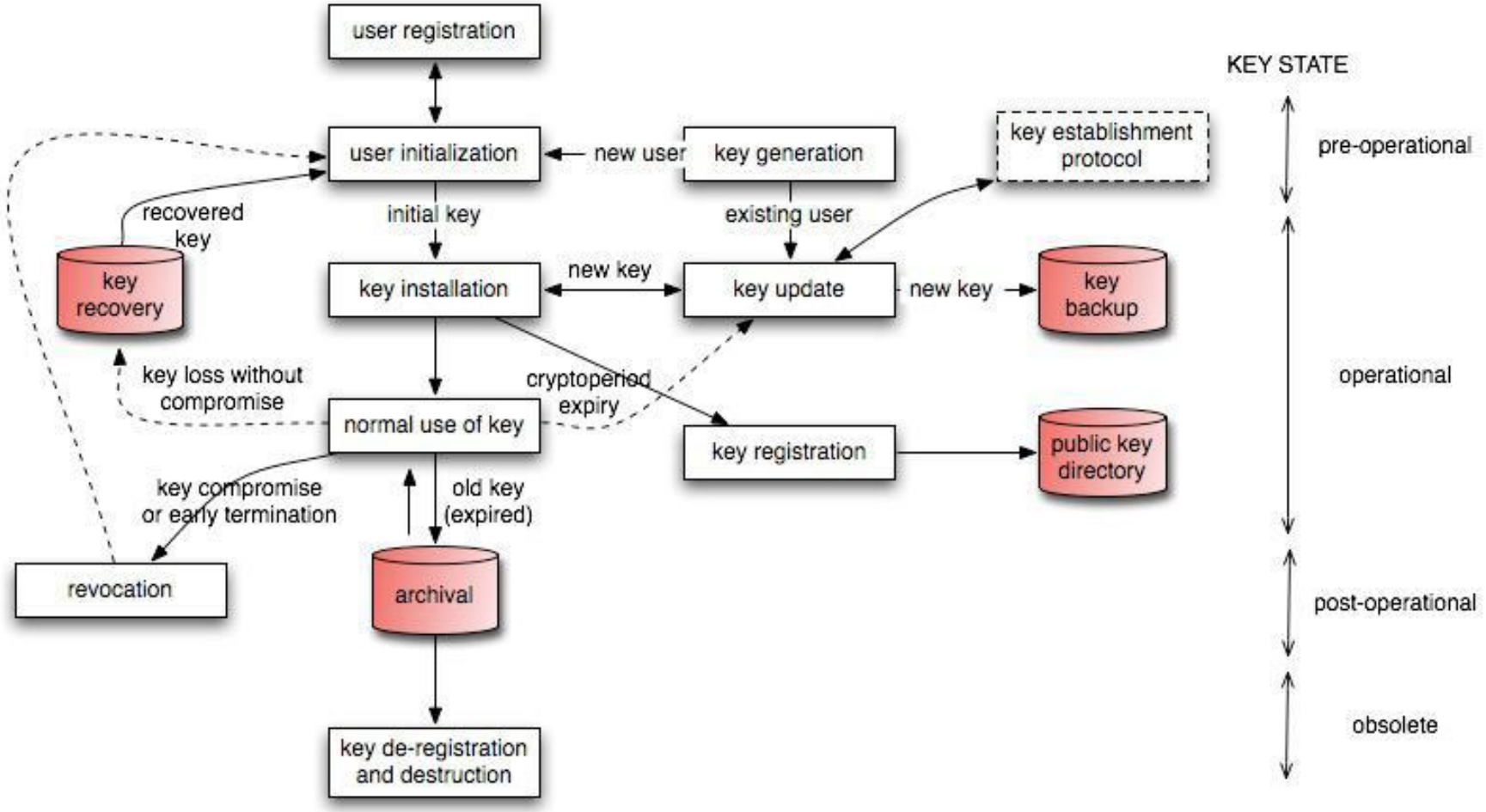
Segurança em Sistemas Informáticos

Gestão de Chaves – Ciclo de vida das chaves

- Estados do ciclo de vida incluem:
  - Registo de Utilizador
  - Inicialização do Utilizador e do Sistema
  - Geração de Chaves
  - Instalação de Chaves
  - Registo de Chaves
  - Utilização Normal
  - Backup de Chaves
  - Actualização de Chaves
  - Arquivo
  - De-registo e destruição de chaves
  - Recuperação de Chaves
  - Revogação de Chaves.

Segurança em Sistemas Informáticos

Gestão de Chaves – Ciclo de vida das chaves



PALMELA
Edifício ATEC · Parque Industrial da Volkswagen Autoeuropa
2950-557 · Quinta do Anjo
Tel. 212 107 300 | info@atec.pt

PORTO
Edifício Siemens · Av. Mário Brito (EN107), nº 3570 · Freixieiro
4456-901· Perafita
Tel. 220 400 500 | infoporto@atec.pt

www.atec.pt