

# Introdução à segurança

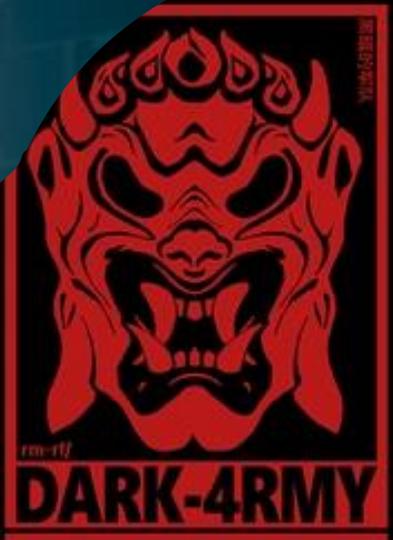
# Segurança ?



```
8b .d8888. .d88b. .o88b. d888888b d88888b d888888b  
88' YP .8P Y8. d8P Y8 `88' 88 88  
`8bo. 88 88 8P 88 8800000 88  
`Y8b. 88 88 8b 88 88  
db 8D `8b d8`Y8b d8 .88. 88. 88.  
'8888Y`Y88P`Y88P`Y888888P Y88888P YP
```

```
{1}--Venom  
{2}--sqlmap  
{3}--Shellnoob  
  --commix  
  --FTP Auto Bypass  
  --jboss-autopwn  
  Blind SQL Automatic Injection And Exploit  
  -uteforce the Android Passcode given the hash  
  mla SQL injection Scanner
```

^ To Main Menu



# Segurança Informática

**Disciplina que se foca na previsibilidade de sistemas,  
processos, ambientes...**

- **Envolve todos os aspectos do ciclo de vida:**
  - Planeamento
  - Desenvolvimento
  - Execução
  - Processos
  - Pessoas
  - Clientes e Fornecedores
  - Mecanismos
  - Normas
  - Propriedade intelectual, ...

# Segurança: planeamento

**Desenho de uma solução que responda aos requisitos,  
num contexto normativo**

- **Sem falhas**

- Todos os estados de funcionamento são previstos
- Não existem estados que fujam à lógica pretendida
  - Mesmo que se usem transições forçadas

- **Respondendo ao ambiente normativo**

- Específico de cada atividade ou setor
- Ex: ISO 27001, ISO 27007, ISO 37001

# Segurança: desenvolvimento

**Implementação uma solução que responda ao design, sem outros modos de funcionamento**

- **Sem erros (bugs) que comprometam a execução correta**
  - Sem “crashes”
  - Sem respostas inválidas ou inesperadas
  - Com tempo de execução correto
  - Com um consumo de recursos adequado
  - Sem fugas de informação
- **Software:**
  - Envolve uma implementação cuidada
  - Envolve testes de forma a se obter uma solução que faça o pretendido... e apenas o pretendido

# Segurança: execução

**Execução de um código tal como foi escrito e com todos os processos previstos**

- **Ambiente controlado, não manipulável, não observável**
- **Sem a existência de comportamentos anómalos, introduzidos pelo ambiente onde executa**
  - Aspetos relevantes: velocidade dos discos, quantidade de RAM, comunicações fiáveis, ...



## ISO 27001 – Clean Desk Policy



# Segurança: pessoas, parceiros

**Comportamento dos sujeitos não possui um impacto negativo na solução**

- Existem normas que definem qual o comportamento correto
- Possuem formação para distinguir quais os comportamentos corretos e incorretos
- Possuem os incentivos para manter comportamentos
- Quando comprometidos ou desviantes, as ações têm um impacto limitado

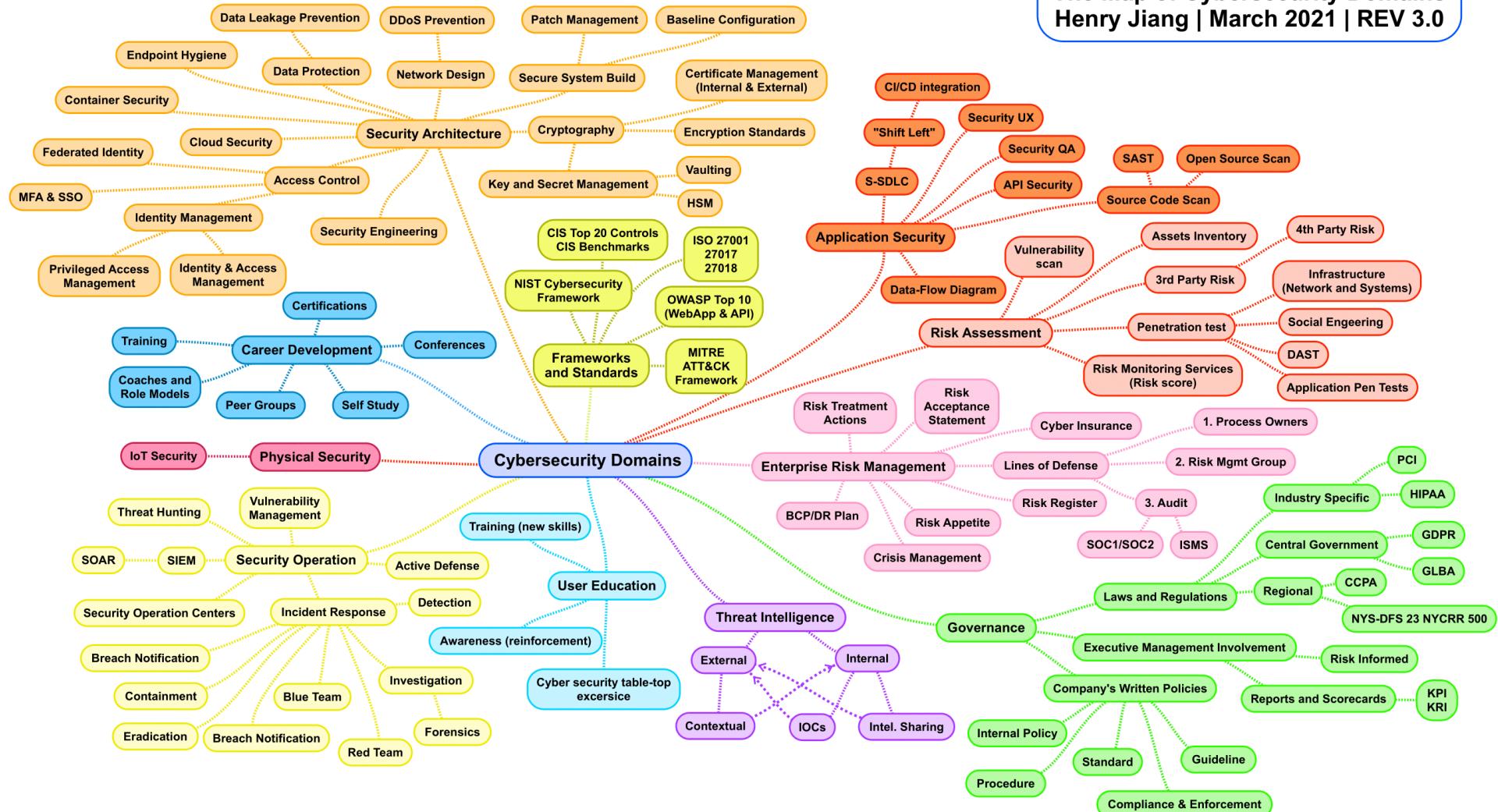
# Segurança: análise e auditoria

**Qual é o comportamento atual da solução?**

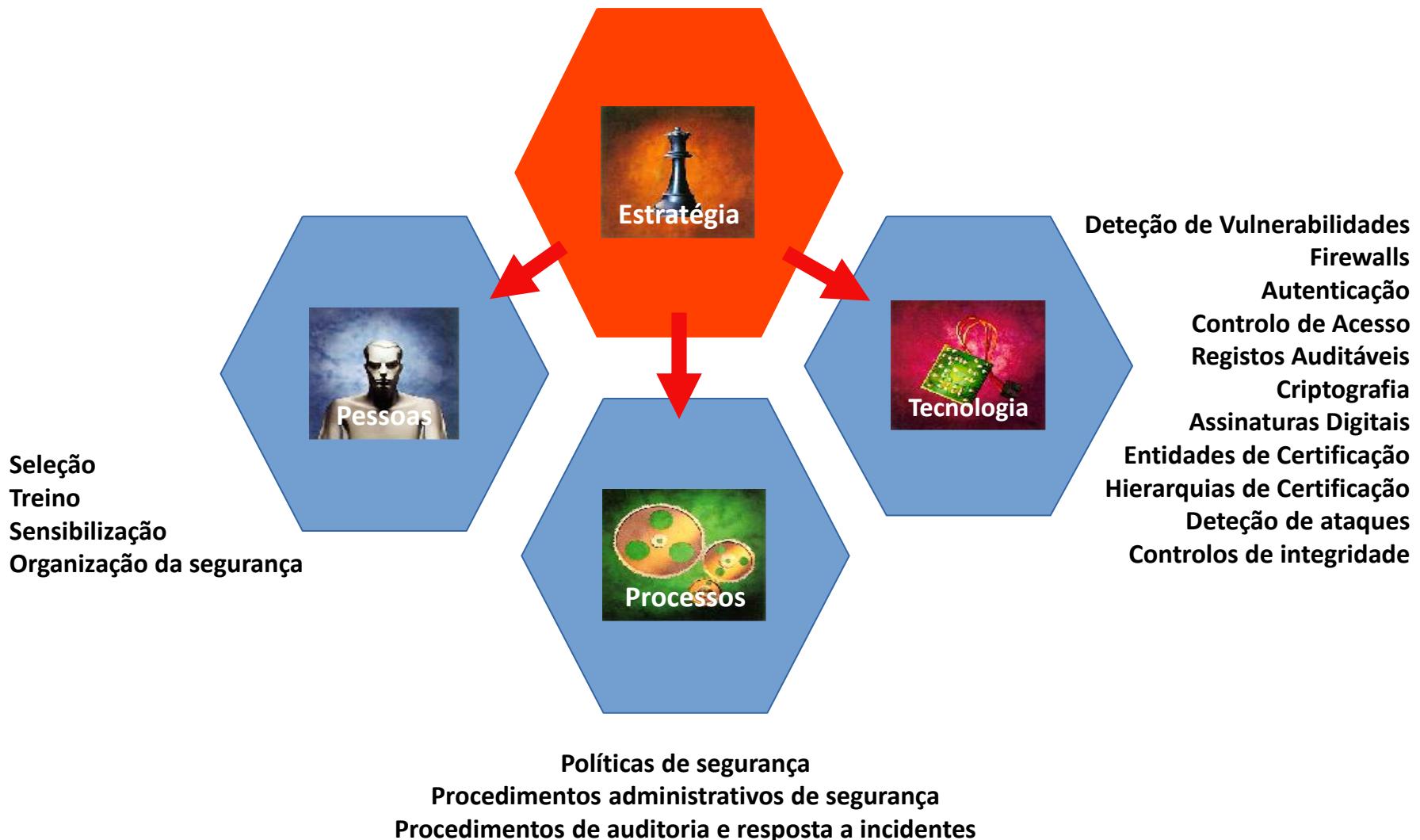
- **Identificar aspectos desviantes**
  - Falhas, erros, comportamentos
- **Identificar o risco da solução ser desviada**
  - Exposição a possíveis atacantes
  - Incentivos para que seja desviada
  - Potenciais atores
- **Identificar o impacto dos desvios**
  - Perda total dos dados? Disrupção? Custo de Operação?

# The Map of Cybersecurity Domains

Henry Jiang | March 2021 | REV 3.0



# Dimensões a considerar

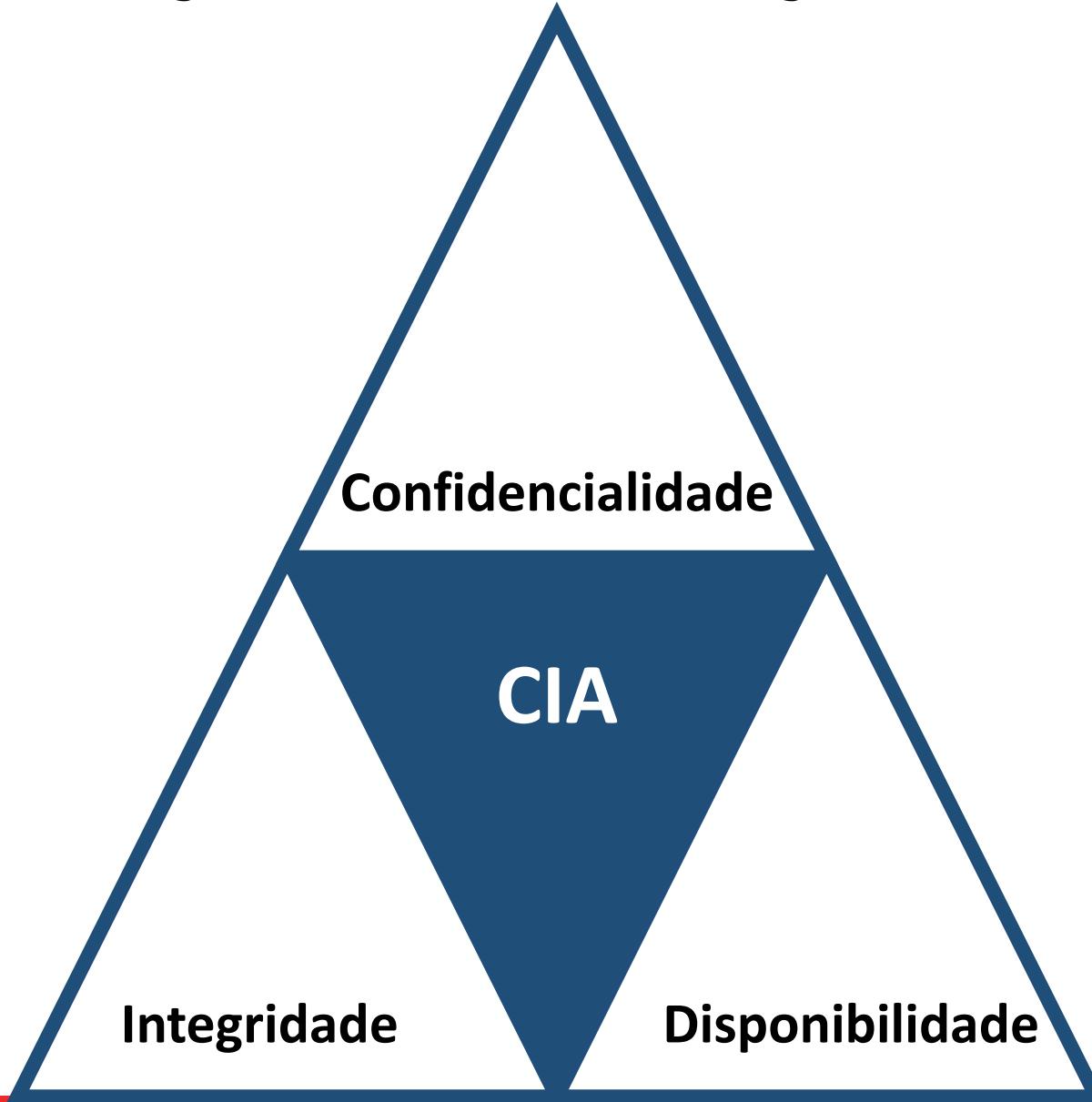


# Facetas

**Facetas da segurança são interligadas e indissociáveis**

- **Defensiva:** foca-se na manutenção da previsibilidade
- **Ofensiva:** foca-se na violação da previsibilidade
  - Pode ter intuito malicioso/criminoso
  - Pode ter intuito de validação da solução (Red Teams)
- **Outras:**
  - **Engenharia Reversa:** recuperação de design a partir do produto
  - **Forense:** identificar ações passadas e recuperar informação
  - **Recuperação de Desastres:** minimizar impacto
  - **Auditoria:** validar o cumprimento com certas premissas

# Segurança da Informação



# Segurança da Informação

- **Confidencialidade:** Informação só pode ser acedida por um grupo restrito de sujeitos
- **Medidas:**
  - Cifrar informação
  - Usar senhas de acesso (fortes)
  - Sistemas de Identificação e Autenticação
  - Firewalls, Grupos de segurança
  - Portas, Paredes robustas
  - Pessoal de Segurança
  - Formação das pessoas

# Segurança da Informação

- **Integridade:** Informação mantém-se inalterada
  - Pode ser aplicada a comportamentos de dispositivos e serviços
- **Medidas:**
  - Controlos de integridade (sínteses)
  - Backups
  - Controlos de Acesso
  - Dispositivos de armazenamento robustos
  - Processos de verificação da informação

# Segurança da Informação

- **Disponibilidade:** Informação mantém-se disponível
  - Pode ser aplicada a serviços e dispositivos
  - Inglês: Availability
- **Medidas:**
  - Backups
  - Planos de recuperação de desastres
  - Redundância
  - Virtualização
  - Monitorização

# Segurança da Informação - também

- **Privacidade: como é tratada a informação pessoal**
  - Recolha
  - Processamento
  - Armazenamento
  - Partilha de informação
  - Eliminação
- **Medidas:**
  - Controlos de acesso
  - Transparência dos processos
  - Cifras
  - Controlos de integridade e de autenticidade
  - Registos

# Objetivos da Segurança (1/3)

- **Defesa contra catástrofes**
  - Fenómenos naturais
  - Temperatura anormal, relâmpagos, picos de energia, inundações, radiação...
- **Degradação dos sistemas informáticos físicos**
  - Setores degradados
  - Falha da fonte de alimentação
  - Erros em células da RAM ou SSD...

# Objetivos da Segurança (2/3)

- **Defesa contra falhas e erros comuns**
  - Falhas de energia
  - Falhas internas aos sistemas operativos
    - Linux Kernel Panic, Windows Blue Screen, OSX panic
    - Bloqueios
    - Consumo anormal de recursos
  - Erros no Software / Erros nas Comunicações

# Objetivos da Segurança (3/3)

- **Defesa contra atividades não autorizadas (adversários)**
  - Iniciados por alguém “de dentro”, ou “de fora”
- **Tipos de atividades não autorizadas:**
  - Acesso a informação
  - Alteração de informação
  - Utilização de recursos
    - CPU, memória, impressão, rede...
  - Negação de serviço (DoS)
  - Vandalismo
    - Interferência do funcionamento normal, sem benefício direto para o atacante

# **Conceitos Fundamentais**

**1. Domínios**

**2. Políticas**

**3. Mecanismos**

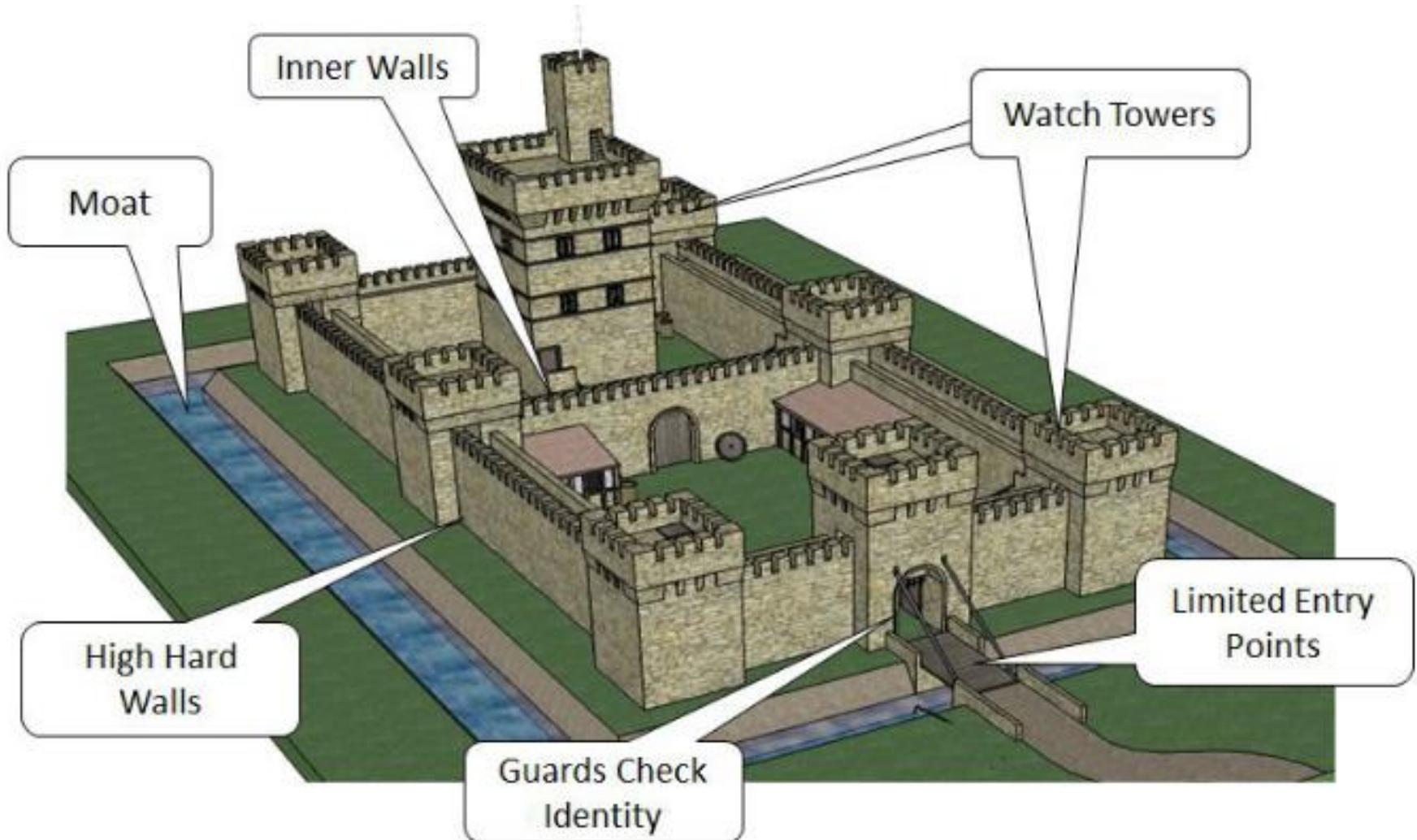
**4. Controlos**

# Domínios de Segurança

**Um conjunto de entidades que partilham atributos de segurança semelhantes**

- **Servem para gerir a segurança de forma agregada**
  - Definem-se os atributos ao domínio
  - Englobam-se entidades no domínio
- **Comportamentos e interações são homogéneos dentro do domínio**
- **Domínios podem ser organizados de forma plana ou hierárquica**
- **Interações entre domínios são normalmente controladas**

# Domínios de Segurança



# Políticas de Segurança

**Conjunto de orientações relativas à segurança que regem um domínio**

- **Organização possui uma hierarquia de políticas**
  - Aplicáveis a cada domínio particular
  - Podem existir sobreposições (ex, hierarquias)
  - Podem possuir âmbitos e níveis de abstração distintos
- **Devem ser coerentes entre si**
- **Exemplo de políticas**
  - Só é possível aceder a serviços web
  - Pessoas têm de se identificar para entrar
  - Paredes devem ser robustas
  - Comunicações devem ser confidenciais

# Políticas de Segurança

- **Definem o poder de cada sujeito**
  - princípio do privilégio mínimo: cada sujeito só tem acesso ao essencial para as suas funções
- **Definem os procedimentos de segurança**
  - quem faz o quê e quando
- **Definem requisitos mínimos de seg. dos sistemas**
  - Níveis de segurança,
  - Grupos de segurança
  - Autorizações e autenticação correspondentes (fraca/forte, simples/multifatorial, remota/presencial)

# Políticas de Segurança

- **Definem a estratégias de defesa e de resposta**
  - Arquitetura defensiva
  - Monitoria de atividades críticas/deteção de sinais de ataques
  - Reação a ataques ou outras disruptões
- **Definem o que é correto e incorreto (legal/ilegal)**
  - Modelo baseado numa lista de negações
    - Proíbem-se algumas coisas
    - O resto é permitido
  - Modelo baseado numa lista de permissões
    - Proíbe-se tudo
    - Algumas coisas são permitidas

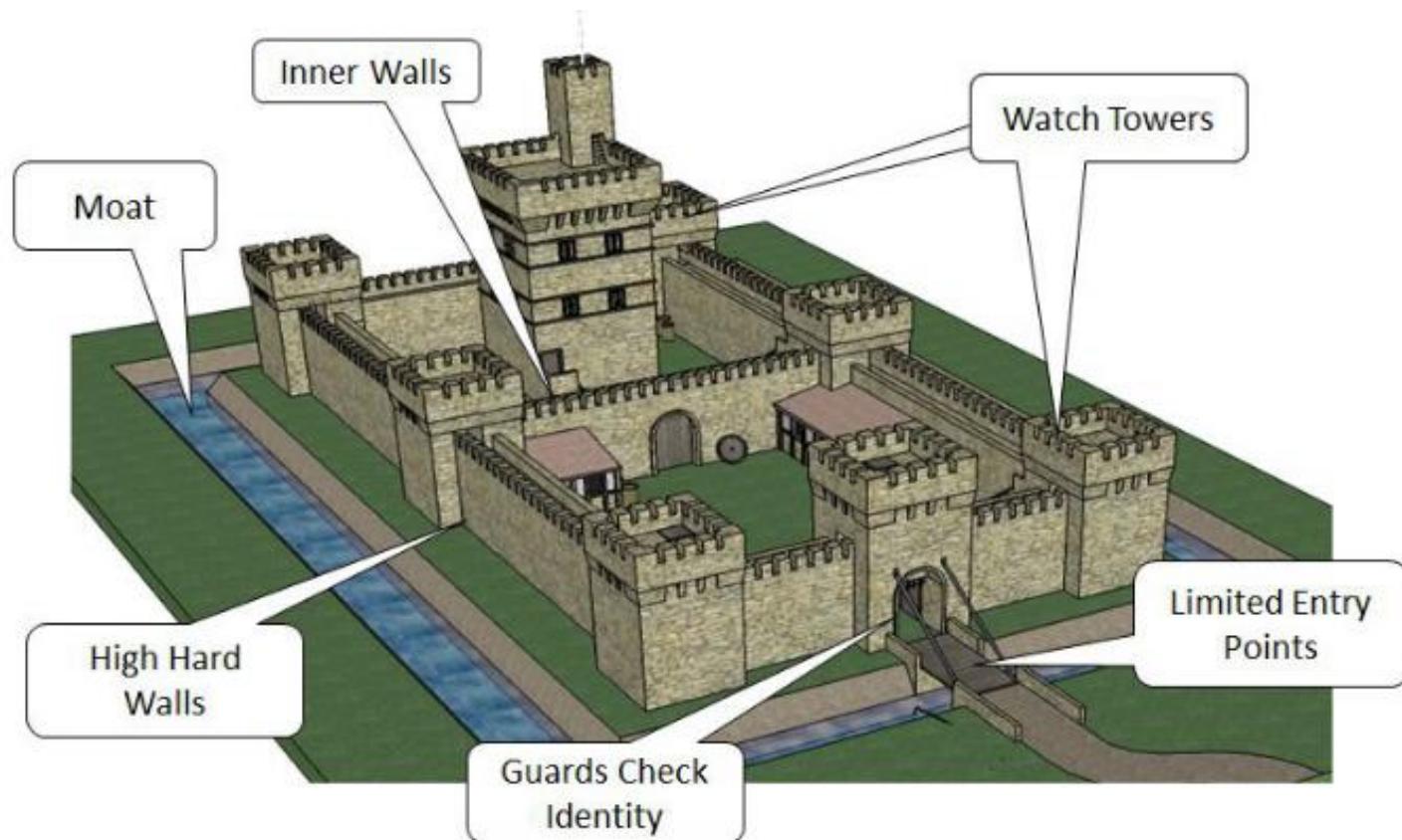
# Mecanismos de Segurança

- **Mecanismos implementam as políticas no domínio**
  - Mecanismos tornam as políticas efetivas no context do domínio
- **Mecanismos de segurança genéricos:**
  - Confinamento
  - Autenticação
  - Controlo de acesso
  - Execução Privilegiada
  - Filtragem
  - Registo
  - Algoritmos e protocolos criptográficos
  - Auditorias
  - Cifras

# Mecanismos de Segurança

**Política:** Movimentos entre domínios devem ser restritos

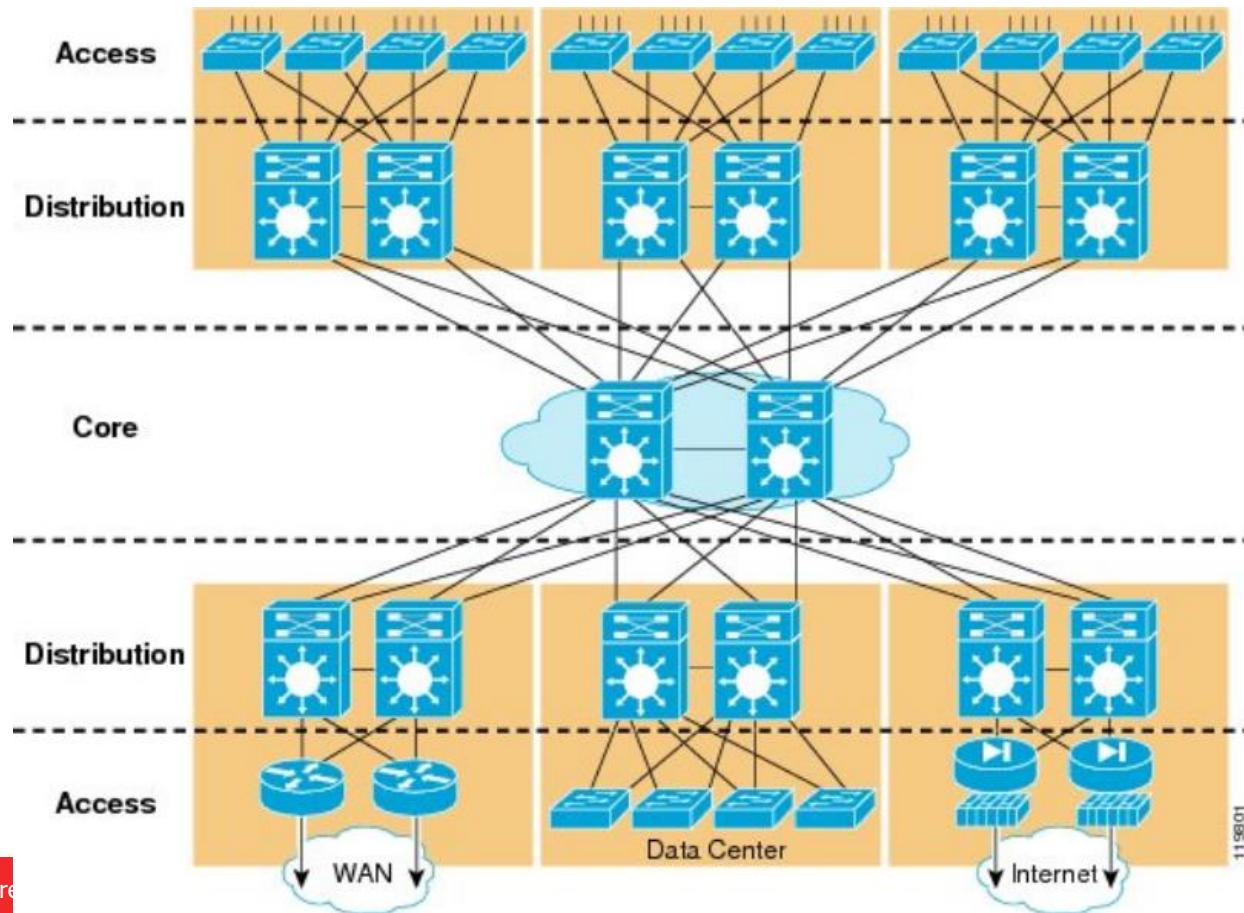
**Mecanismos:** Portas, guardas, senhas, objetos/documentos



# Mecanismos de Segurança

**Política:** Sistemas devem ser resilientes

**Mecanismos:** Equipamentos/ligações duplicadas, arquitetura



11901

# Controlos de Segurança

**Controlos são todos e quaisquer aspetos que permitam evitar, detetar, neutralizar ou minimizar o risco**

- **Controlos incluem políticas e mecanismos, mas também:**
  - Normas e Leis
  - Processos
  - Políticas
  - Mecanismos
  - Técnicas, etc...
- **Controlos são definidos de forma explícita e são verificáveis**
  - Exemplo: ISO 27001 define 114 controlos em 14 grupos
    - ... Gestão de equipamentos, segurança física, gestão de incidentes...

# Tipos de Controlos

	Prevenção	Deteção	Correção
<b>Físicos</b>	<ul style="list-style-type: none"><li>- Vedações</li><li>- Portões</li><li>- Fechaduras</li></ul>	<ul style="list-style-type: none"><li>- CCTV</li></ul>	<ul style="list-style-type: none"><li>- Reparar fechaduras</li><li>- Reparar janelas</li><li>- Reemitir cartões de acesso</li></ul>
<b>Técnicos</b>	<ul style="list-style-type: none"><li>- Firewall</li><li>- Autenticação</li><li>- Antivírus</li></ul>	<ul style="list-style-type: none"><li>- Deteção de intrusões</li><li>- Alarmes</li><li>- Honeypots</li></ul>	<ul style="list-style-type: none"><li>- Correção de vulnerabilidades</li><li>- Reiniciar sistemas</li><li>- Repor VMs</li><li>- Remover Vírus</li></ul>
<b>Administrativos</b>	<ul style="list-style-type: none"><li>- Cláusulas Contratuais</li><li>- Separação de obrigações</li><li>- Classificação de Informação</li></ul>	<ul style="list-style-type: none"><li>- Revisão de matrizes de acesso</li><li>- Auditorias</li></ul>	<ul style="list-style-type: none"><li>- Implementar planos de continuidade de negócio</li><li>- Implementar plano de resposta a incidentes</li></ul>

# Tipos de Controlos

	Prevenção	Deteção	Correção
Físicos	<ul style="list-style-type: none"><li>- Vedações</li><li>- Portões</li><li>- Fechaduras</li></ul>	<ul style="list-style-type: none"><li>- CCTV</li></ul>	<ul style="list-style-type: none"><li>- Reparar fechaduras</li><li>Reparar janelas</li></ul>
Técnicos	<ul style="list-style-type: none"><li>- Firewall</li><li>- Autenticação</li><li>- Antivírus</li></ul>		
Administrativos	<ul style="list-style-type: none"><li>- Cláusulas Contratuais</li><li>- Organização</li><li>- Classificação Informação</li></ul>		

**Amarelo: em relação a um evento**

**Vermelho: de acordo com a característica**

# Aplicação da Segurança

## Prevenção realista

- Considerar que não existe segurança perfeita
- Focar nos eventos mais prováveis
  - Poderá depender da localização física, enquadramento legal,...
- Considerar custo e receitas
  - Um grande número de controlos tem um custo baixo
  - Custo de uma estratégia de segurança não tem limite prático
- Considerar todos os domínios e entidades
  - Um ataque numa entidade pode comprometer outras lateralmente

# Aplicação da Segurança

## Prevenção realista

- **Considerar impacto**
  - À luz da CIA, ou outros aspectos relevantes (e.g Marca)
- **Considerar custo e tempo de recuperação**
  - Custo monetário, reputação, posição de mercado
- **Caracterizar os atacantes**
  - E criar controlos para esses atacantes
  - Existem sempre atacantes com mais conhecimento/recursos
- **Considerar que o sistema vai ser comprometido**
  - Ter planos de recuperação

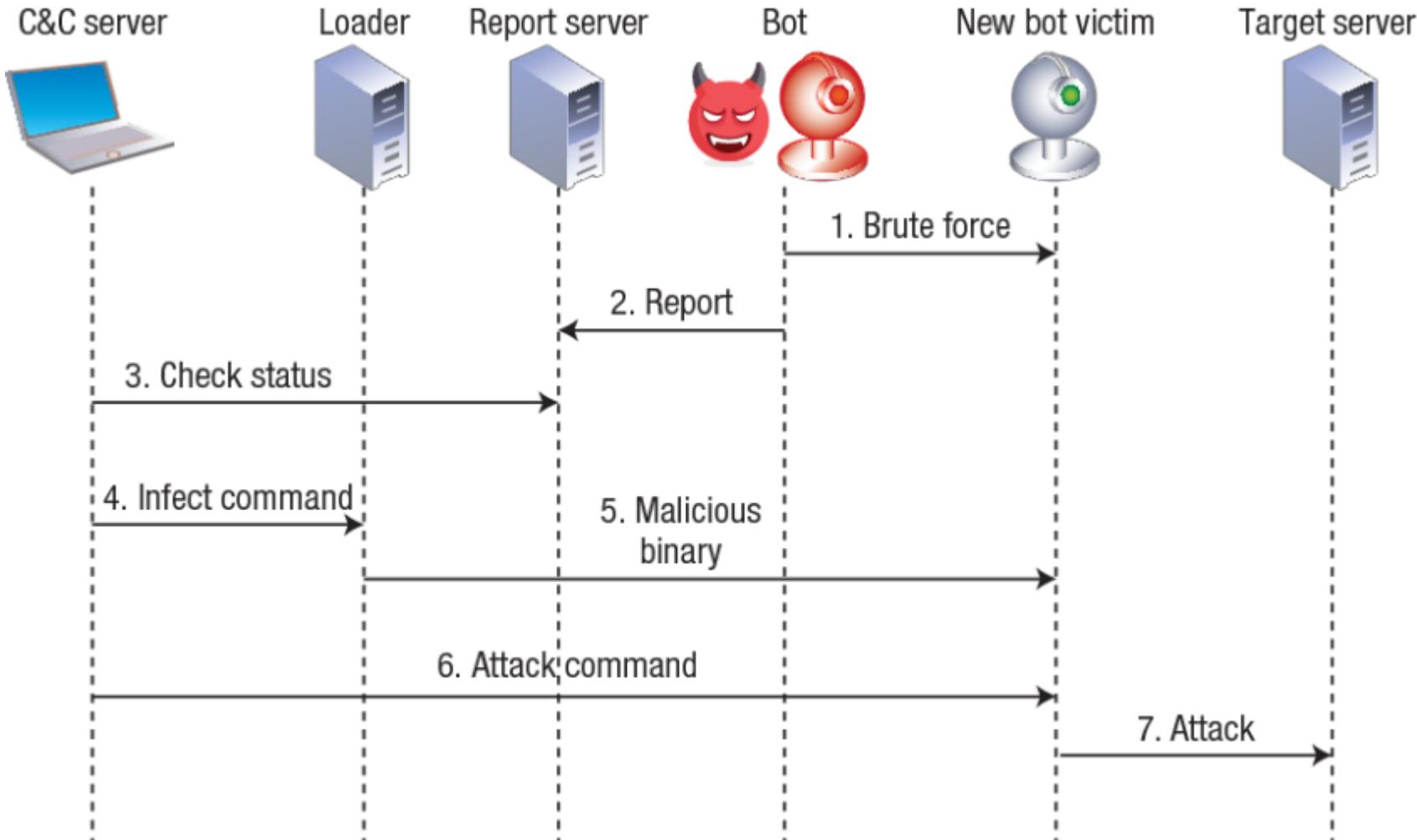
# Segurança nos Sistemas Computacionais: Problema Complexo

- **Computadores podem fazer muitos estragos num curto espaço de tempo**
  - Podem processar grandes quantidades de informação
  - Processam informação a grande velocidade
- **O número de vulnerabilidades aumenta sempre**
  - Complexidade incremental dos sistemas
  - Pressões de mercado (time to market, ou custo)

# Segurança nos Sistemas Computacionais: Problema Complexo

- **Redes permitem novos mecanismos de ataque**
  - Ataques anónimos de qualquer ponto do planeta
  - Ataques distribuídos sobre várias geografias
  - Exploração de aplicações e sistemas inseguros
- **Atacantes podem construir cadeias de ataque complexas**
  - Primeira exploração
  - Movimento lateral
  - Exfiltração de informação
  - Etc...<https://attack.mitre.org/matrices/enterprise/>

# Encadeamento de atividades



Operação e comunicação da botnet Mirai botnet.

Mirai causa uma negação de serviço distribuída (DDoS) a servidores, propagando-se constantemente para dispositivos IoT mal configurados

Fonte: Kolias, Constantinos et al. "DDoS in the IoT: Mirai and Other Botnets." Computer 50, 2017: 80-84

# Segurança nos Sistemas Computacionais: Problema Complexo

- **Usuários não possuem noção do risco**
  - Não conhecem o problema
    - ... o impacto
    - ... as boas práticas
    - ... ou as soluções
- **Usuários são desleixados**
  - Tomam riscos
  - Não querem saber (não possuem/identificam responsabilidade)
  - Não estimam o risco de forma adequada

# Principais fontes de Vulnerabilidades

- **Aplicações hostis ou erros em aplicações**
  - Root kits: Inserem elementos no Sistema Operativo
  - Worms: Programas controlados por um atacante
  - Vírus: Código executável p/ infetar ficheiros (ex, Macros)
- **Usuários**
  - Ignorantes e descuidados
    - ... telnet vs ssh, FTP vs FTPS, IMAP vs IMAPS, HTTP vs HTTPS
  - Falsa noção de segurança (ex: tenho um anti-vírus, estou protegido)
  - Hostis
- **Administração deficiente**
  - A configuração por omissão raramente é a mais segura
  - Restrições de Segurança vs Operações Flexíveis
  - Exceções a indivíduos
- **Comunicações sobre ligações não controladas/conhecidas**

# Políticas de Segurança em Sistemas Distribuídos

**Tem de englobar múltiplos sistemas e redes**

- **Domínios de segurança**
  - Definição de um conjunto de sistemas e rede
  - Definição de um conjunto de usuários aceites/autorizados
  - Definição de um conjunto de atividades aceites/não aceites
- **Gateways de segurança**
  - Definição das interações de entrada e saída de um domínio
- **Conjunto de controlos para validação**

# Defesa em Perímetro

(mínimo aconselhado, **mas insuficiente**)

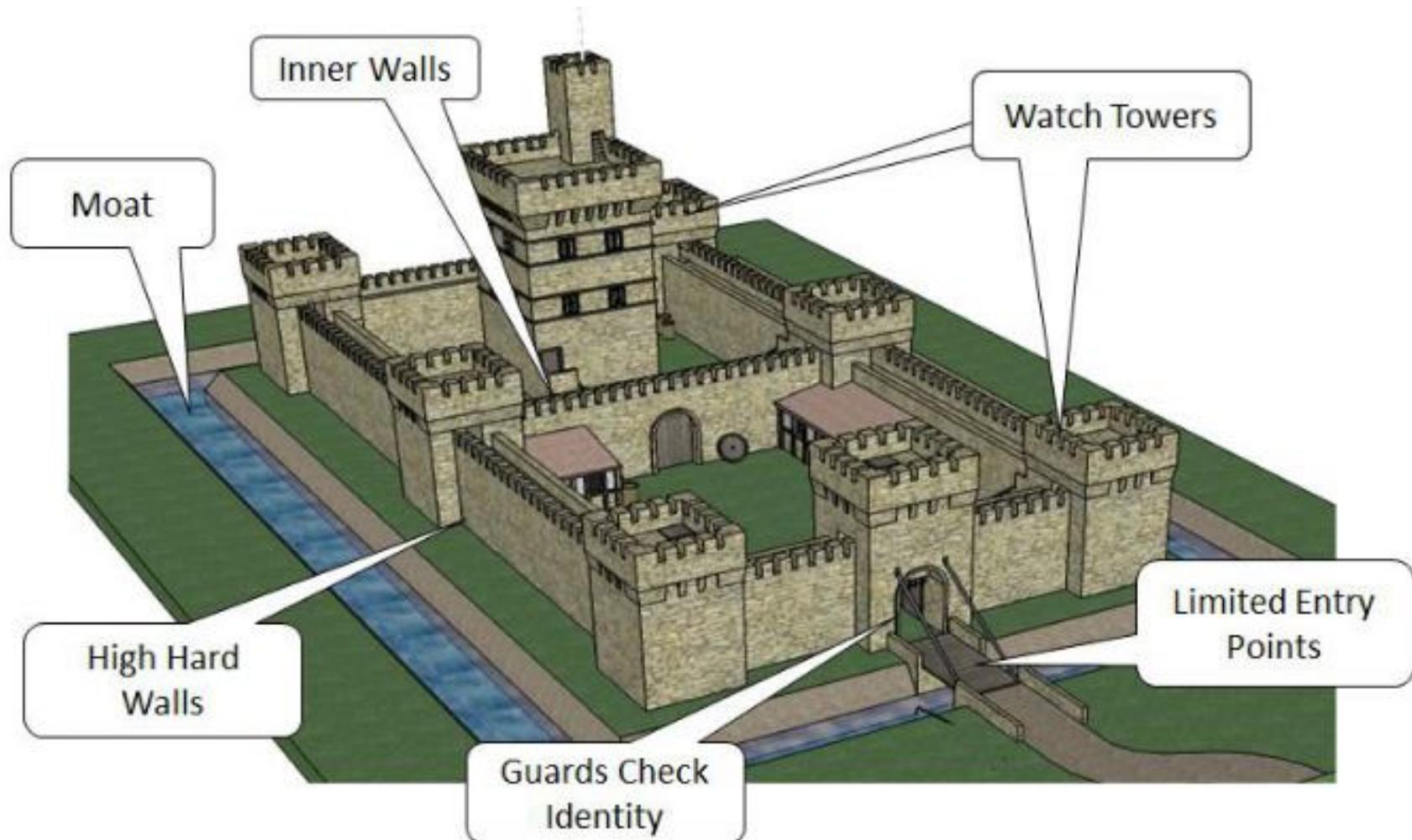


# Defesa em Perímetro

- **Proteção contra atacantes externos**
  - Internet
  - Outros utilizadores
  - Outra organização
- **Assume que utilizadores internos são confiáveis e partilham políticas**
  - Amigos, família, colaboradores
- **Utilização doméstica ou em pequenas organizações**
- **Limitações**
  - Não protege contra atacantes internos
    - Utilizadores de confiança
    - Atacantes que adquiriram acesso interno

# Defesa em profundidade

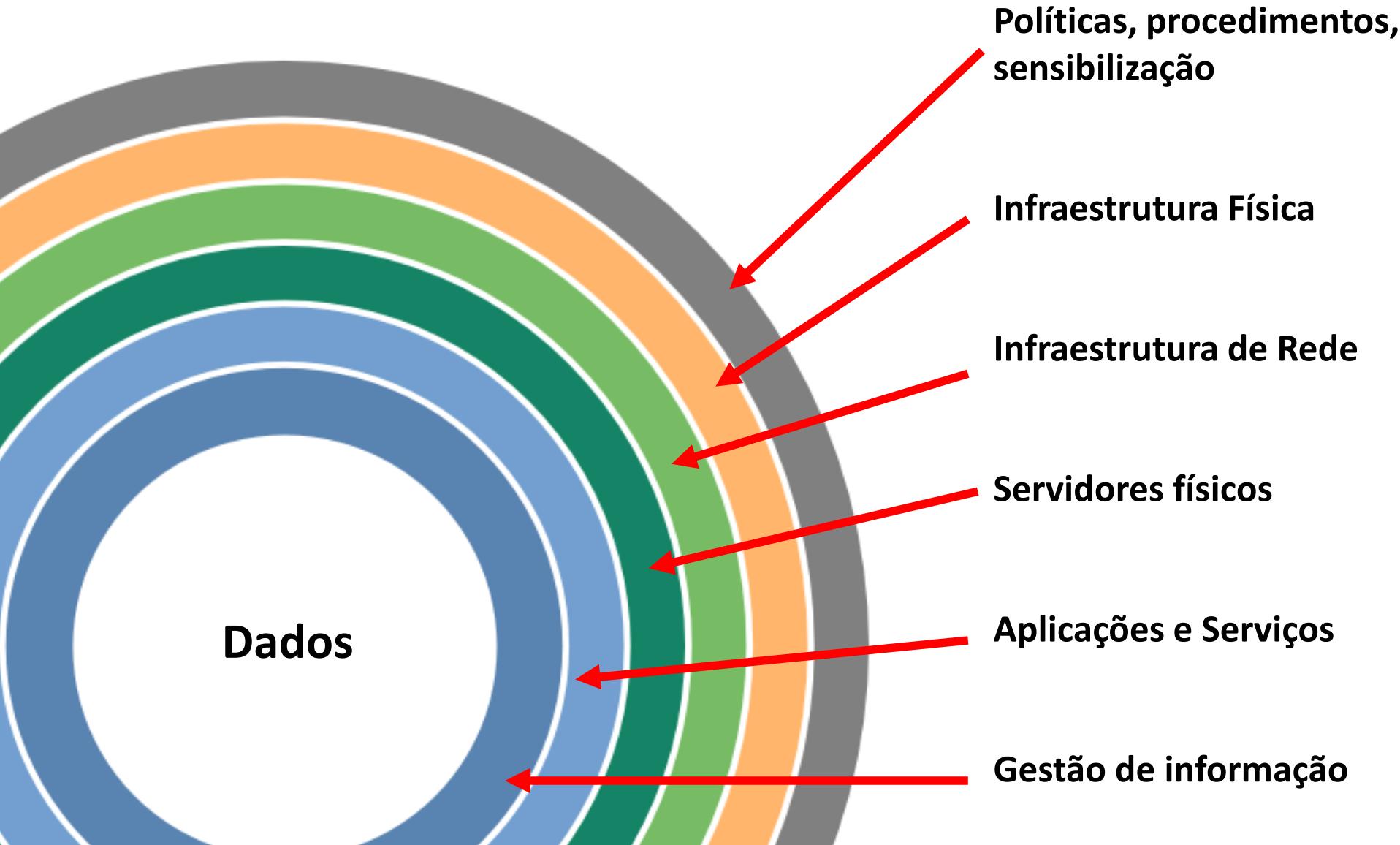
(mais adequado, mas também falível)



# Defesa em Profundidade

- **Proteção contra atacantes externos e internos**
  - Internet
  - Qualquer utilizador
  - Outra organização
- **Assume domínios bem definidos sobre todos os aspetos**
  - Paredes, Portas blindadas, autenticação, vigilantes, cifras, redes seguras...
- **Limitações**
  - Necessária uma coordenação entre controlos
    - Possível acumulação de controlos, com sobreposição de funções mas também buracos na defesa
  - Custo
  - Necessidade de Treino, alteração de processos e auditorias frequentes

# Defesa em profundidade



# Defesa em profundidade

- **Sistemas Operativos Confiáveis**
  - Níveis de segurança, certificação
  - Ambientes de execução segura
  - Sandboxes / Máquinas Virtuais
- **Firewalls e Sistemas de segurança**
  - Controlo de tráfego entre redes
  - Monitorização (carga de tráfego, comportamento...)
- **Comunicações Seguras / VPNs**
  - Canais seguros sobre redes públicas / inseguras
  - Extensão segura das redes da organização

# Defesa em profundidade

- **Autenticação**
  - Local
  - Remota (sobre a rede)
  - Single Sign-On
  - Segredos, Tokens, biometria, dispositivos, localização
- **Entidades de Certificação /PKI**
  - Gestão de chaves públicas e certificados
- **Cifra de ficheiros e dados em sessões**
  - Privacidade/confidencialidade de dados transmitidos
  - Privacidade/confidencialidade de dados armazenados

# Defesa em profundidade

- **Deteção de intrusões**
  - Deteção de atividades proibidas ou anómalas
  - Baseado na rede / baseado nos sistemas
- **Inventariação de vulnerabilidades**
  - Pesquisa para resolução de problemas ou exploração
  - Baseado na rede / baseado no sistemas
- **Testes de Penetração**
  - Avaliação das vulnerabilidades
  - Demonstração de tentativas de penetração
  - Teste de mecanismos de segurança instalados
  - Determinação da existência de políticas de segurança mal aplicadas

# Defesa em profundidade

- **Monitorização de conteúdos**
  - Deteção de vírus, Worms e outras ciber-pragas
- **Administração da segurança**
  - Desenvolvimento de políticas de segurança
  - Aplicação das políticas de forma distribuída
  - Co-administração / contratação de equipas externas
- **Resposta a Incidentes / Seguimento em Tempo Real**
  - Capacidade para detetar e reagir a incidentes em tempo real
  - Meios para resposta rápida e efetiva a incidentes

# Zero Trust

- **Modelo de defesa sem perímetros específicos**
  - Não existe confiança intrínseca por entidades serem internas
    - Aliás, pode não existir definição de interno ou externo
- **Modelo recomendado para novos sistemas**
  - Sistemas tradicionais deverão migrar para este modelo
  - Implica o desenho de sistemas/serviços para este modelo
  - Sistemas legados requerem a instalação de níveis adicionais de proteção
    - Firewalls, filtros, adaptadores, plugins,...

# Zero Trust – Princípios (NCSC)

## 1. Conhecer a arquitetura

- serviços, dispositivos, pessoas

## 1. Conhecer as identidades

- pessoas, serviços e saúde dos dispositivos

## 2. Validar comportamentos e saúde de dispositivos e serviços

## 3. Usar políticas para autorizar pedidos

# Zero Trust – Princípios (NCSC)

## 5. Autenticar e autorizar todas as interações

- Nada de APIs abertas, ou restritas por endereço IP

## 6. Monitorizar utilizadores, dispositivos e serviços

## 7. Não confiar em nenhuma rede, nem mesmo a própria

- Atacantes internos deverão ter o mesmo acesso que os externos

## 8. Usar serviços desenvolvidos para Zero Trust

### 5. Serviços legados

# Atualidade – Utilizadores comuns

- **Usam os mesmos dispositivos para todas as suas interações**
  - Contactar outros
  - Aceder a serviços de lazer
  - Aceder a serviços críticos (ex., Bancos)
  - Trabalho (?)
- **Utilização de sistemas e serviços com base no objetivo final**
  - Comprar, aceder, ver, ouvir, comunicar
- **Sem formação e incautos**
  - Maus a calcular risco das suas ações
  - Consideram que os problemas só acontecem a grandes empresas/outros
    - Consideram que não são importantes
  - Com ideias pré-concebidas erradas
    - “algoritmos” para gerar senhas, reutilização de senhas
  - Sem investimento em segurança (exceto o eventual antivírus)
    - Consideram que o antivírus fornece proteção total
  - Sem processos de recuperação de incidentes

# Atualidade - Empresas

- **Focadas no objeto do negócio**
  - Produto que fornecem
  - Aspetos financeiros
  - Recursos Humanos
- **Seguras na medida do estritamente necessário**
  - Devem cumprir regras e ambientes normativos
    - RGPD, regulação específica dos setores
  - Podem ter estratégias de segurança
    - Desde nada até serem focadas em “security driven culture”
  - Podem fornecer treino e investir em segurança
  - Podem ter auditorias frequentes
  - Podem ter um CISO: Chief Information Security Officer

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a “necessary evil.”	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. Decentralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

*Source: Enterprise Strategy Group, 2014.*

# Atualidade - Nações

- **Focadas na soberania política, económica, cultural**
  - Agindo de forma independente ou concertada (ex., NATO)
- **Possuem entidades dedicadas à cibersegurança**
  - Ciber defesa
    - Parte integrante das forças armadas
    - Entidades ad-hoc contratadas ou não declaradas
  - Ciber resiliência das entidades da nação
    - Universidades, utilities, empresas, cidadãos
    - Entidades específicas: Centro Nacional de Cibersegurança
  - Investigação criminal
    - Polícias
- **Podem realizar ações ofensivas contra outras entidades**
  - Empresas, indivíduos, grupos, nações
  - Guerra fria, governos totalitários, soberania

# Atualidade – Grupos ofensivos

- **Realizam ataques contra qualquer um**
  - De forma esporádica ou concertada
  - Podem possuir grandes fundos disponíveis
    - Financiamento por grupos económicos ou nações
  - Podem agir como um coletivo sem organização estrita
- **Por vezes considerados Advanced Persistent Threats (APT)**
  - Realizam ataques ao longo de meses/anos
  - Podem manter-se numa entidade de forma silenciosa
- **Variadas motivações**
  - Hacktivismo: Lulzsec, Anonymous, AntiSec, (4chan?)
  - Concorrência económica
  - Interesses nacionais: Advanced Persistent Threats (APTs)
  - Crime: APTs, grupos variados de ransomware
  - Ciberguerra

# Atualidade – Grupos Criminosos

- **Frequentemente operam como empresas**
  - Modelo de negócio explícito
  - Empregados e outros colaboradores
  - “Linha de suporte” (para ajudar vítimas a pagar resgates)
  - Por vezes com presença publica e publicidade
- **Operam segundo vários modelos**
  - Podem operar de países que os “ignoram”
    - E não atacam sistemas nesses países
  - Operações por contrato (outras empresas, nações, ...)
  - Dirigidos a uma base de utilizadores larga ou outras companhias
  - Foco em áreas de negócio específicas (infraestruturas críticas, saúde, banca...)
- **Ambiente de software rico e dinâmico**
  - Software especificamente desenvolvido para estas atividades
    - Explorando vulnerabilidades em sistemas
    - Vulnerabilidades são comercializadas e são ferramentas para incluir nos ataques a sistemas
  - Podem fazer uso de ferramentas automáticas ou software dirigido

# Fatores Limitantes

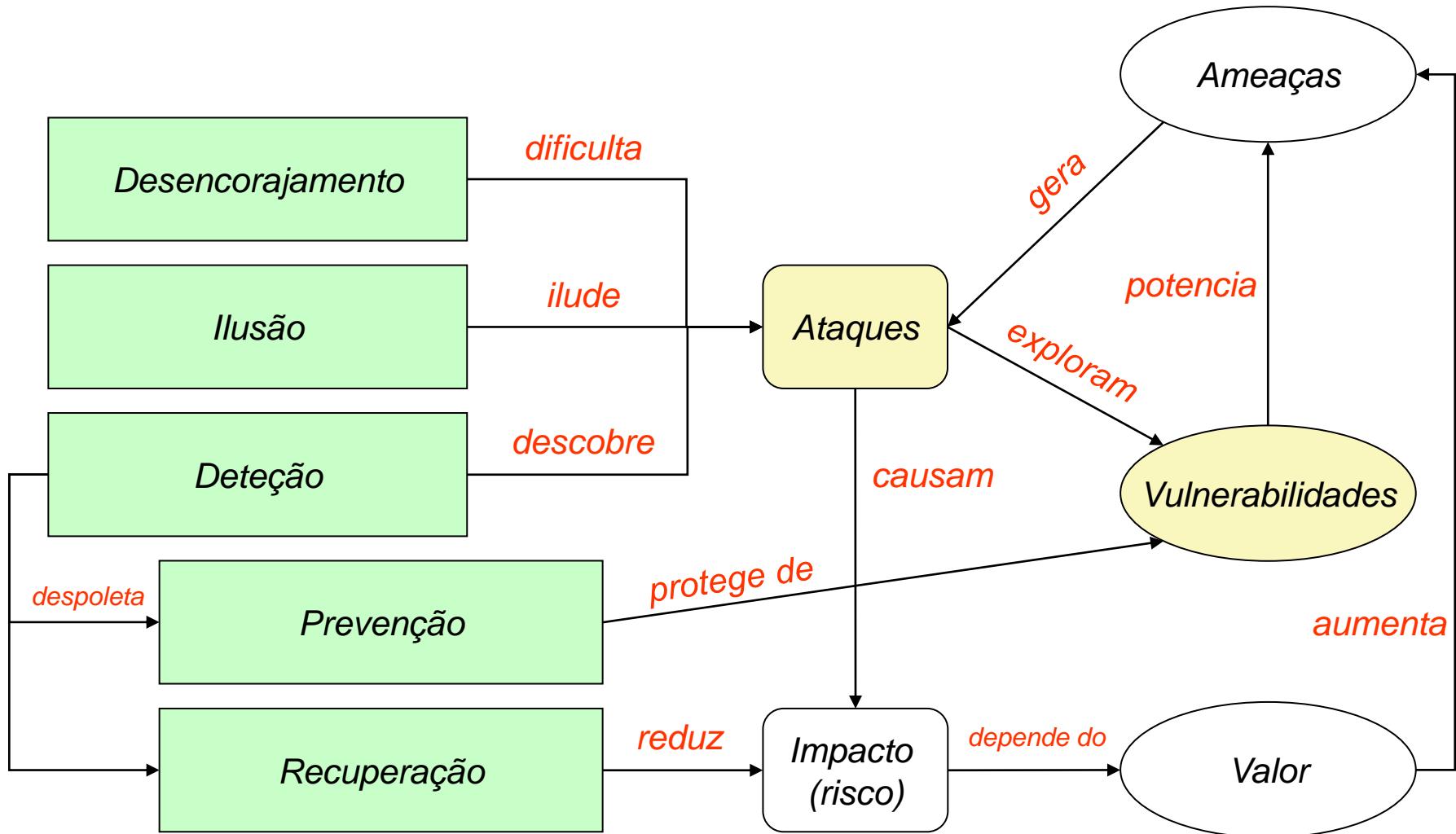
- Cibersegurança é limitada por aspectos económicos, operacionais e logísticos
  - Todas as entidades possuem recursos limitados
- Cibersegurança resume-se a construir e aplicar uma estratégia, com um orçamento e num contexto operacional e legal

<http://targetedattacks.trendmicro.com/cyoa/en/>



# Vulnerabilidades

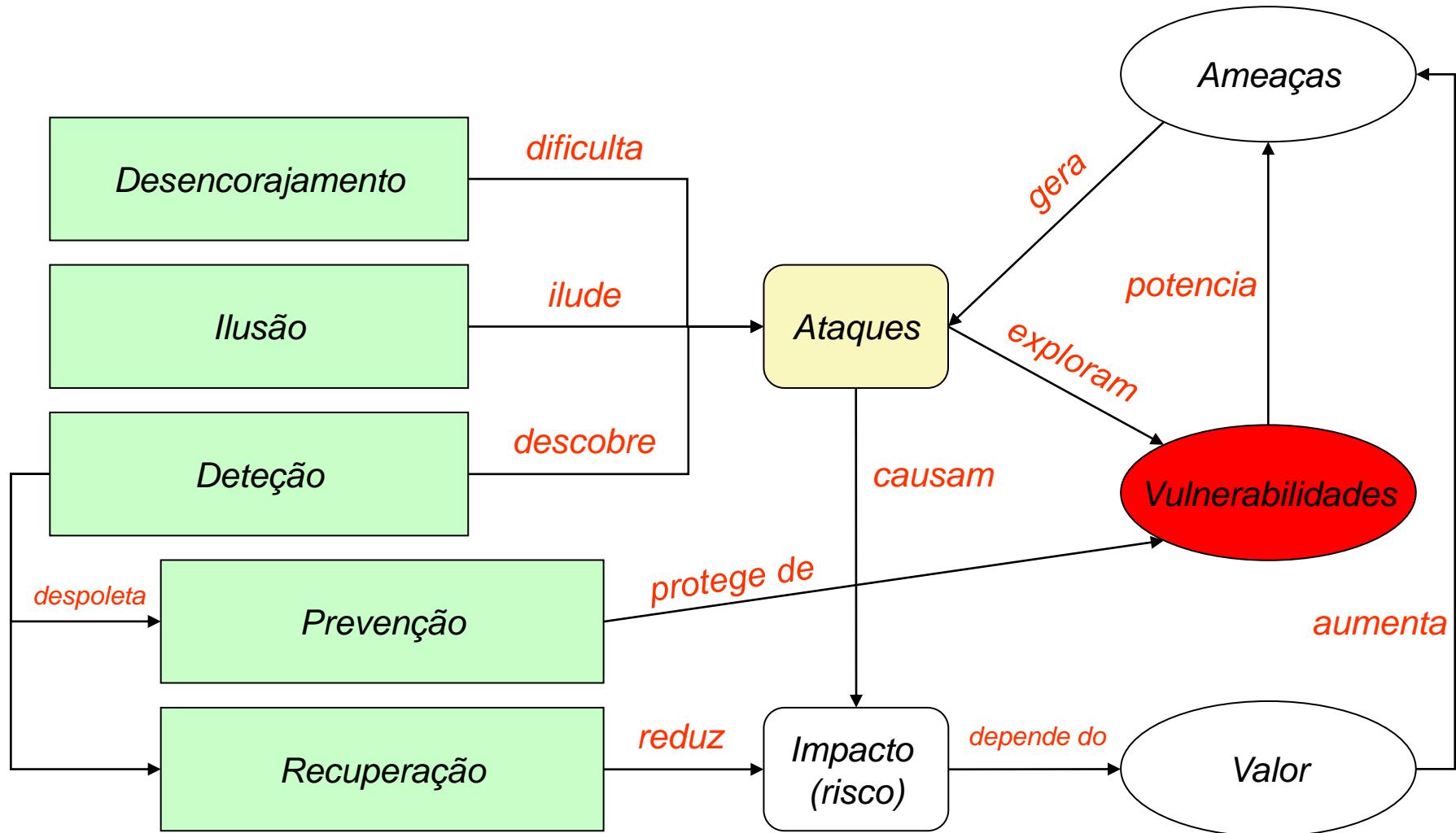
# Segurança da Informação



# Medidas (e algumas ferramentas)

- **Desencorajamento**
  - Punição
    - Restrições legais
    - Provas forenses
  - Barreiras de Segurança
    - Firewalls
    - Autenticação
    - Comunicação Segura
    - Sandboxing
- **Deteção**
  - Sistemas de Deteção de Intrusões
    - ex: Snort, Zeek, Suricata
  - Auditorias
  - Análise Forense
- **Ilusão**
  - Honeypots /Honeynets
  - Acompanhamento Forense
- **Prevenção**
  - Políticas restritivas
    - ex: privilégio mínimo
  - Deteção de vulnerabilidades
    - ex: OpenVAS, metasploit
  - Correção de Vulnerabilidades
    - ex: atualizações regulares
- **Recuperação**
  - Backups
  - Sistemas redundantes
  - Recuperação forense

# Segurança da Informação



# Vulnerabilidade

**Erro no software que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede**

- **Um erro só é uma vulnerabilidade se permitir que o atacante viole uma política de segurança**
  - Exclui políticas de segurança “abertas” onde todos os utentes são de confiança ou onde não se considera a existência de riscos para o sistema
- **Um vulnerabilidade é um estado de um sistema que permite:**
  - que um atacante execute comandos em nome de terceiros
  - que um atacante aceda a dados ultrapassando as restrições de acesso
  - que o atacante se apresente como outrem
  - que o atacante negue a prestação de serviços

# Exposição

**Problema de configuração de um sistema ou um erro no software que permitem aceder a informação ou capacidades que podem auxiliar um atacante**

- **Não permite comprometer diretamente um Sistema/rede**
  - Mas é uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável
- **Uma exposição é um estado de um sistema que:**
  - permite que um atacante realize recolhas de informação
  - permite a um atacante esconder as suas atividades
  - Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
  - É um ponto de entrada comum para atacantes obterem acesso
  - É considerado problemático por uma política de segurança razoável

# Prontidão (Security Readiness)

- **Medidas de Desencorajamento, Ilusão e Detecção endereçam maioritariamente vulnerabilidades conhecidas**
  - Tentativas de reconhecimento (ex: Port Scanning)
  - Ataques genéricos (ex: Interceção de redes)
  - Ataques específicos (ex: Buffer Overflows)
- **Medidas de Prevenção endereçam vulnerabilidades conhecidas e desconhecidas**
  - Vulnerabilidades genéricas
    - ex: reação a respostas mal formadas (protocol scrubbers)
    - ex: ataques furtivos (normalização para formatos canónicos)
  - Vulnerabilidades específicas
    - ex: erro de particular de software (testes e validação)

# Prontidão (Security Readiness)

A aplicação das medidas requer conhecimento específico

- **Vulnerabilidades conhecidas**
  - Problema, forma de exploração, impacto, etc.
- **Padrões de atividade dos ataques**
  - Modus operandi
  - Assinaturas de ataques
- **Padrões anormais de atividade**
  - Anormal é o oposto de normal...
    - ... mas o que é que é normal?
  - Difícil de definir em ambientes heterogéneos

source: [flickr](#)



1  
DEVICE



1 Year Subscription  
Abonnement d'un an

Includes Antivirus Security  
Comprend la protection  
antivirus

100%

**GUARANTEE / GARANTIE  
DE PROTECTION COMPLÈTE\***

Viruses removed or your money back  
Éradication des virus garantie ou argent remis

Always updated to the latest version  
Une protection toujours dotée de la version la plus récente



Internet Connection Required  
Connexion Internet requise

# Prontidão (Security Readiness)

- **As ameaças em redes de computadores são diferentes de outros tipos de ameaças**
  - Os ataques podem ser lançados em qual hora, de qualquer local
  - Podem ser facilmente coordenados
    - Ex. Distributed Denial of Service attacks (DDoS)
  - Possuem um baixo custo de execução
  - Podem ser automatizados
  - São rápidos
- **Portanto, requerem uma capacidade permanente (24x7) de reação a ataques:**
  - Equipas de especialistas em segurança
  - Alertas de ataque na hora
  - Teste e avaliação dos níveis de segurança existentes
  - Procedimentos de reação expeditos

# CVE: Common Vulnerabilities and Exposures

- **Dicionário público de vulnerabilidades e exposições**
  - Para gestão de vulnerabilidades
  - Para gestão de correções (patches)
  - Para alarmística de vulnerabilidades
  - Para deteção de intrusões
- **Utiliza identificadores comuns para um mesmo CVE**
  - Permite a troca de informações entre produtos de segurança
  - Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços
- **Detalhes de um CVE podem ser privados**
  - Parte do processo de divulgação responsável: espera-se que o fornecedor crie uma correção

**CVE-ID****CVE-2015-1538**[Learn more at National Vulnerability Database \(NVD\)](#)[CVSS Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#) • [CPE Information](#)**Description**

Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.

**References**

**Note:** [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:76052
- [URL: http://www.securityfocus.com/bid/76052](http://www.securityfocus.com/bid/76052)
- [CONFIRM: http://www.huawei.com/en/psirt/security-advisories/hw-448928](http://www.huawei.com/en/psirt/security-advisories/hw-448928)
- [CONFIRM: http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm](http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm)
- [CONFIRM: https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398](https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398)
- EXPLOIT-DB:38124
- [URL: https://www.exploit-db.com/exploits/38124/](https://www.exploit-db.com/exploits/38124/)
- [MISC: http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html](http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html)
- MLIST:[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)
- [URL: https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fl6RQM/yzJvoTVrIQAJ](https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fl6RQM/yzJvoTVrIQAJ)
- SECTRACK:1033094
- [URL: http://www.securitytracker.com/id/1033094](http://www.securitytracker.com/id/1033094)

**Assigning CNA**

MITRE Corporation

**Date Entry Created****20150206**

Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

**Phase (Legacy)**

Assigned (20150206)

**Votes (Legacy)****Comments (Legacy)****Proposed (Legacy)**

N/A

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

**SEARCH CVE USING KEYWORDS:**  You can also search by reference using the [CVE Reference Maps](#).**For More Information:** [CVE Request Web Form](#) (select "Other" from dropdown)

# CVE: Identificadores

Aka CVE names, CVE numbers, CVE-IDs, or CVEs

- **Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List**
  - Estados possíveis: "candidate" ou "entry"
  - **Candidate:** sob revisão para inclusão na CVE List
  - **Entry:** aceite na CVE List
- **Formato**
  - Identificador numérico CVE (CVE-Ano-Índice)
  - Estado (candidate ou entry)
  - Descrição sumária da vulnerabilidade ou exposição
  - Referências para informação adicional

# Benefícios dos CVEs

**Fornece uma linguagem comum para referir problemas**

- **Facilita a partilha de dados entre**
  - Sistemas de deteção de intrusões
  - Ferramentas de aferição
  - Bases de dados de vulnerabilidades
  - Investigadores
  - Equipas de resposta a incidentes
- **Permite melhorar as ferramentas de segurança**
  - Maior abrangência, facilidade de comparação, interoperabilidade
  - Sistemas de alarme e reporte
- **Fomenta a inovação**
  - Local primordial para discutir conteúdos críticos das BDs

# CVEs e Ataques



- **Ataques podem usar várias vulnerabilidades**
  - Um CVE para cada vulnerabilidade em todos os sistemas
- **Exemplo: Stagefright (Android, video em mensagens MMS)**
  - CVE-2015-1538, P0006, Google Stagefright 'stsc' MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright 'ctts' MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright 'stts' MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright 'stss' MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1539, P0007, Google Stagefright 'esds' MP4 Atom Integer Underflow Remote Code Execution
  - CVE-2015-3827, P0008, Google Stagefright 'covr' MP4 Atom Integer Underflow Remote Code Execution
  - CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
  - CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
  - CVE-2015-3824, P0011, Google Stagefright 'tx3g' MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-3829, P0012, Google Stagefright 'covr' MP4 Atom Integer Overflow Remote Code Execution

# Deteção de Vulnerabilidades

- **Ferramentas podem detetar vulnerabilidades**
  - Exploram vulnerabilidades conhecidas
  - Testam padrões de vulnerabilidades
    - ex. buffer overflow, SQL injection, XSS, etc.
- **Ferramentas podem replicar ataques conhecidos**
  - Utilizam exploits conhecidos para vulnerabilidades conhecidas
    - ex: MS Samba v1 utilizado no WannaCry
  - Permitem implementar correções mais rapidamente
- **Vitais para aferir a robustez das aplicações e sistemas em operação**
  - Serviço frequentemente contratado

# Deteção de Vulnerabilidades

- **Podem ser aplicadas a:**
  - Código desenvolvido (análise estática)
    - OWASP LAPSE+, RIPS, Veracode, ...
  - Aplicação a executar (análise dinâmica)
    - Valgrind, Rational, AppScan, GCC, ...
  - Externamente como um sistema remoto
    - OpenVAS, Metasploit, ...
- **Não devem ser aplicadas cegamente a sistemas em produção!**
  - Potencial perda/corrupção de dados
  - Potencial negação de serviço
  - Potencial ato ilegal

# CWE: Common Weakness Enumeration

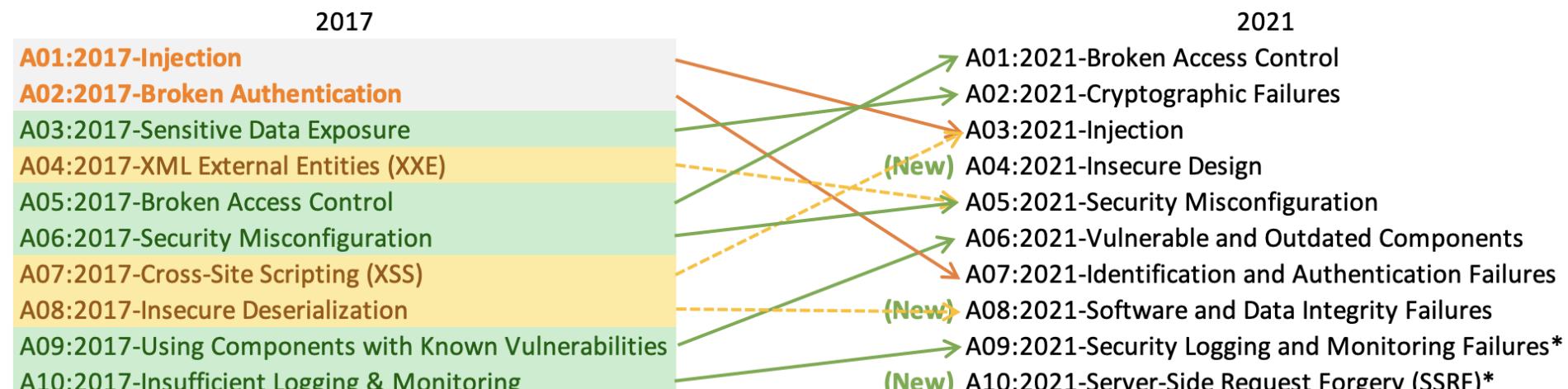
- **Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança**
  - De programas, do seu desenho ou da arquitetura de sistemas
  - Cada CWE representa um tipo de vulnerabilidade
  - Gerida pela MITRE Corporation
  - Esta lista fornece uma definição pormenorizada de cada CWE
- **Os CWEs são catalogados segundo uma estrutura hierárquica**
  - CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidade
    - Podem ter vários CWEs filhos associados
  - CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
    - Com menos ou sem CWEs filhos

**CWE != CVE**

# Vulnerability sources – OWASP Top 10 (Web)

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulns.
10. Insufficient logging and monitoring

# Tipos de Vulnerabilidades – OWASP Top 10



# CWE-348: Use of Less Trusted Source

**The software has two different sources of the same data or information, but it uses the source that has less support for verification, is less trusted, or is less resistant to attack.**

- Details at: <https://cwe.mitre.org/data/definitions/348.html>
  - Describes pattern, provides examples, provides list of related CVEs

# CWE-348: Use of Less Trusted Source

```
$requestingIP = '0.0.0.0';
if (array_key_exists('HTTP_X_FORWARDED_FOR', $_SERVER)) {
    $requestingIP = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else{
    $requestingIP = $_SERVER['REMOTE_ADDR'];
}

if(in_array($requestingIP,$ipAllowlist)){
    generatePage();
    return;
}
else{
    echo "You are not authorized to view this page";
    return;
}
```

Definido pelo  
servidor Web  
Ou pelo cliente

Definido pelo  
servidor Web

# Análise Estática ( com Sonarcloud)

Reliability [Measures](#)

1.7k E

 Bugs ?

started 11 months ago

Security [Measures](#)

244 E

 Vulnerabilities ?

312

 Security Hotspots ?

Maintainability [Measures](#)

271d A

 Debt ?

15k

 Code Smells ?

Duplications [Measures](#)



3.2%

Duplications ?

2.5k

Duplicated Blocks ?

# Análise Estática ( com Sonarcloud)

The screenshot shows the SonarCloud interface displaying static analysis results for a WordPress plugin. The left sidebar contains navigation links for Status, Security Category (OWASP A...), SonarSource, OWASP Top 10 (A1 - INJECTION), SANS Top 25, and CWE, along with a search bar for CWEs. The main content area lists issues found in wp-admin/includes/plugin.php, wp-admin/plugin-editor.php, wp-content/plugins/wpDiscuz/options/class.WpdiscuzOptions.php, and wp-includes/functions.php. Each issue is detailed with a title, description, severity (Vulnerability, Blocker, Open), status (Not assigned), effort (30min), and a comment link. The interface includes navigation controls for selecting issues and navigating through the results.

wp-admin/includes/plugin.php

Change this code to not use user-controlled data in include statements. [Why is this an issue?](#)

**Vulnerability** **Blocker** **Open** **Not assigned** 30min effort [Comment](#)

11 months ago L1882 [Edit](#) [Delete](#) [No tags](#)

wp-admin/plugin-editor.php

Change this code to not construct the path from user-controlled data. [Why is this an issue?](#)

**Vulnerability** **Blocker** **Open** **Not assigned** 30min effort [Comment](#)

11 months ago L71 [Edit](#) [Delete](#) [No tags](#)

wp-content/plugins/wpDiscuz/options/class.WpdiscuzOptions.php

Change this code to not construct the path from user-controlled data. [Why is this an issue?](#)

**Vulnerability** **Blocker** **Open** **Not assigned** 30min effort [Comment](#)

11 months ago L353 [Edit](#) [Delete](#) [No tags](#)

wp-includes/functions.php

Change this code to not construct the path from user-controlled data. [Why is this an issue?](#)

**Vulnerability** **Blocker** **Open** **Not assigned** 30min effort [Comment](#)

11 months ago L4838 [Edit](#) [Delete](#) [No tags](#)

4 of 4 shown

# Gestão de Vulnerabilidades

- **Durante o ciclo de desenvolvimento, como bugs**
  - Podem ser geridos por equipa de segurança ou de desenvolvimento
- **Quando o software é público, vulnerabilidades são geridas globalmente**
  - Para todos as aplicações disponíveis
- **Gestão pública permite um maior foco**
  - Discussão centrada numa aplicação específica
    - Ex: uma biblioteca específica, usada em vários sistemas
  - Admins podem rapidamente testar os seus sistemas, melhorando a segurança
  - ... Atacantes também ficam a saber melhor como atacar sistemas

# Gestão de Vulnerabilidades

- **Vulnerabilidades também são geridas de forma privada**
  - Constituem arsenais para ataques a alvos no futuro
  - Códigos de ataque (Exploits) podem ser vistos como munições
- **Conhecimento sobre exploits é comercializado**
  - Preços de 0 a 2-3M€ (ou mais?) através de compras diretas
  - Ofertas públicas até 2.5M€ para programas de procura de erros (Google, Zerodium)
    - 2.5M€: 1 click Android exploit
    - 2M€: 1 click iPhone exploit
    - 1.5M€: WhatsApp ou iMessage exploit
    - ~2K por um XSS no HackerOne (existem regtos de \$1M de pagamento)
- **...e trocados de forma privada a preços desconhecidos**
  - Companhias privadas, crime organizado, APTs...

# CVE-2020-1472 @ MITRE

Informação Básica sobre o CVE

Refere outros trackers e páginas com informação

Páginas de fabricantes

Páginas de distribuições

Mailing lists

The screenshot shows a web browser displaying the MITRE CVE database. The URL in the address bar is [cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472). The page header includes the CVE logo and navigation links for CVE List, CNAs, WGs, News & Blog, Board, and About. A sidebar on the right is titled "NVD" with links to CVSS Scores and CPE Info. The main content area shows the details for CVE-2020-1472, including its ID, a brief description of the vulnerability, and a list of references from various sources like CERT, Synology, and Microsoft.

**CVE-ID**  
**CVE-2020-1472** [Learn more at National Vulnerability Database \(NVD\)](#)  
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

**Description**  
An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

**References**  
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CERT-VN:VU#490028
- [URL:https://www.kb.cert.org/vuls/id/490028](https://www.kb.cert.org/vuls/id/490028)
- CONFIRM:[https://www.synology.com/security/advisory/Synology\\_SA\\_20\\_21](https://www.synology.com/security/advisory/Synology_SA_20_21)
- MISC:<http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html>
- MISC:<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>
- URL:<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472>
- MLIST:[oss-security] 20200917 Samba and CVE-2020-1472 ("Zerologon")
- URL:<http://www.openwall.com/lists/oss-security/2020/09/17/2>
- UBUNTU:USN-4510-1
- URL:<https://usn.ubuntu.com/4510-1/>
- UBUNTU:USN-4510-2
- URL:<https://usn.ubuntu.com/4510-2/>

# CVE-2020-1472@NVD

## Informação Básica sobre o CVE

## Uma pequena análise

## Uma pontuação de criticalidade (CVSS)

## The CVE Severity Score

## Ligações a outras páginas

The screenshot shows the NVD Detail page for CVE-2020-1472. The page has a header with the title 'CVE-2020-1472 Detail'. Below the header, there's a 'MODIFIED' status message: 'This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.' The 'Current Description' section contains the following text: 'An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability''. There is a link to 'View Analysis Description'. The 'Severity' section shows 'CVSS Version 3.x' selected. The CVSS 3.x Severity and Metrics section includes an NVD logo, the text 'NIST: NVD', a 'Base Score: 10.0 CRITICAL', and a 'Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/H:H/A:H'. A note below states: 'NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.' Another note says: 'Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.' The 'References to Advisories, Solutions, and Tools' section contains a table with one row. The table has two columns: 'Hyperlink' and 'Resource'. The 'Hyperlink' column contains the URL 'http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html'. The 'Resource' column is empty.

Hyperlink	Resource
<a href="http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html">http://packetstormsecurity.com/files/159190/Zerologon-Proof-Of-Concept.html</a>	

# CVE-2020-1472 @ Microsoft (Vendor)

**Mais detalhe sobre o problema, como aparece, como pode ser resolvido**

**Informação para staff sobre atualizações**

**Informação sobre a existência de exploits públicos**

**Cada fornecedor usa um formato próprio, com níveis de detalhe muito variados.**

The screenshot shows a Microsoft Edge browser window displaying the security advisory for CVE-2020-1472. The URL is [portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472). The page title is "CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability". It includes sections for "Security Vulnerability", "Published: 08/11/2020 | Last Updated : 08/11/2020", and "MITRE CVE-2020-1472". The main content describes the vulnerability as an elevation of privilege issue related to the Netlogon protocol. It mentions that Microsoft is addressing the vulnerability in a phased two-part rollout. A sidebar titled "On this page" lists links to "Executive Summary", "Exploitability Assessment", "Security Updates", "Mitigations", "Workarounds", "FAQ", "Acknowledgements", "Disclaimer", and "Revisions". At the bottom, there's a "Exploitability Assessment" section with a table comparing publicly disclosed information across different software releases.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

Security Updates      CVSS Score

# CVE-2020-1472 @ Em outros locais

**Profissionais (ou não)  
criam provas de  
conceito para explorar  
o problema**

**Podem ser usados para  
validar se um Sistema  
é vulnerável**

**Comunidade ad-hoc e  
muito dinâmica**

The screenshot shows a GitHub repository page for 'VoidSec/CVE-2020-1472: Exploit'. The repository has 4 stars, 97 forks, and 21 contributors. It contains 1 branch and 0 tags. The 'Code' tab is selected, showing a list of files: README.md, research/exploit, .gitignore, README.md, cve-2020-1472-exploit.py, nRPC.py, reinstall\_original\_pw.py, and requirements.txt. The README.md file contains the following content:

```
CVE-2020-1472

Checker & Exploit Code for CVE-2020-1472 aka Zerologon

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

NOTE: It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to
```

The repository also includes sections for About, Releases, Packages, and Languages.

# Gestão de vulnerabilidades

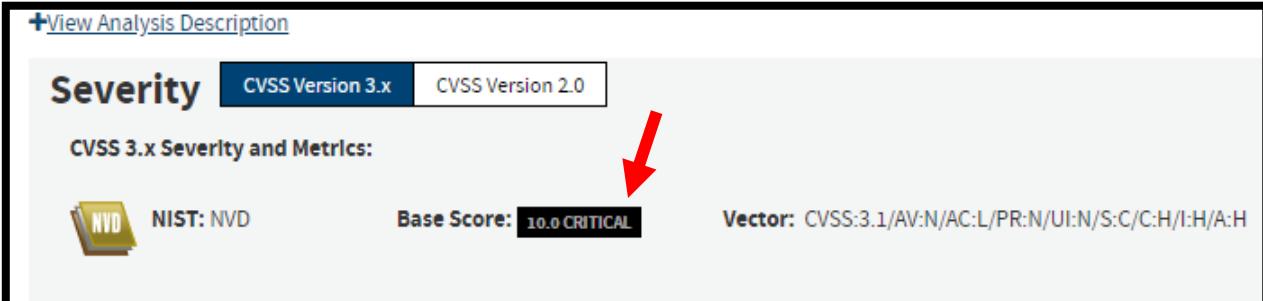
- Tarefa não é simples
- Exploits nem sempre são conhecidos
- Impeto e valor podem ser sub-estimados
- Informação antiga pode levar a um falso sentido de segurança
- Comunidade é muito dinâmica
  - Defensores que podem testar diretamente
  - Atacantes que podem incorporar vulnerabilidades

[+View Analysis Description](#)

**Severity** CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NVD NIST: NVD Base Score: 10.0 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Exploitability Assessment

The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

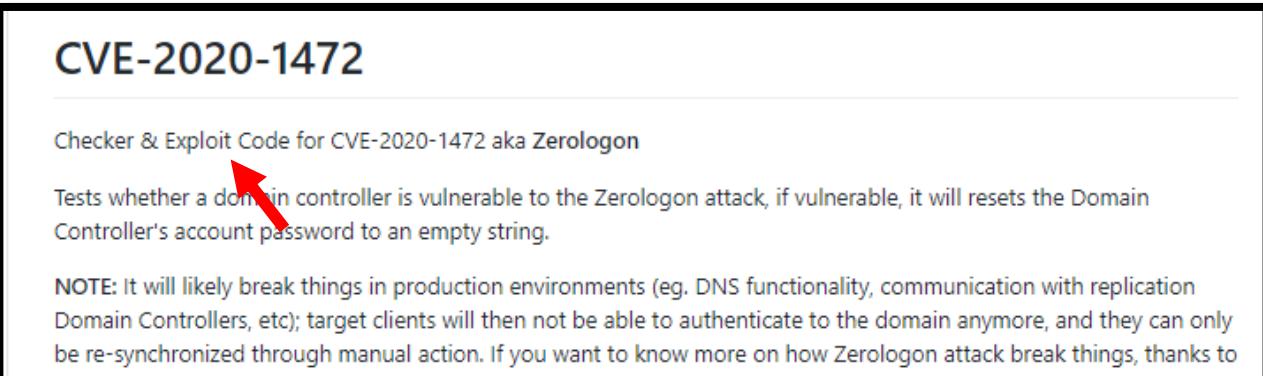


## CVE-2020-1472

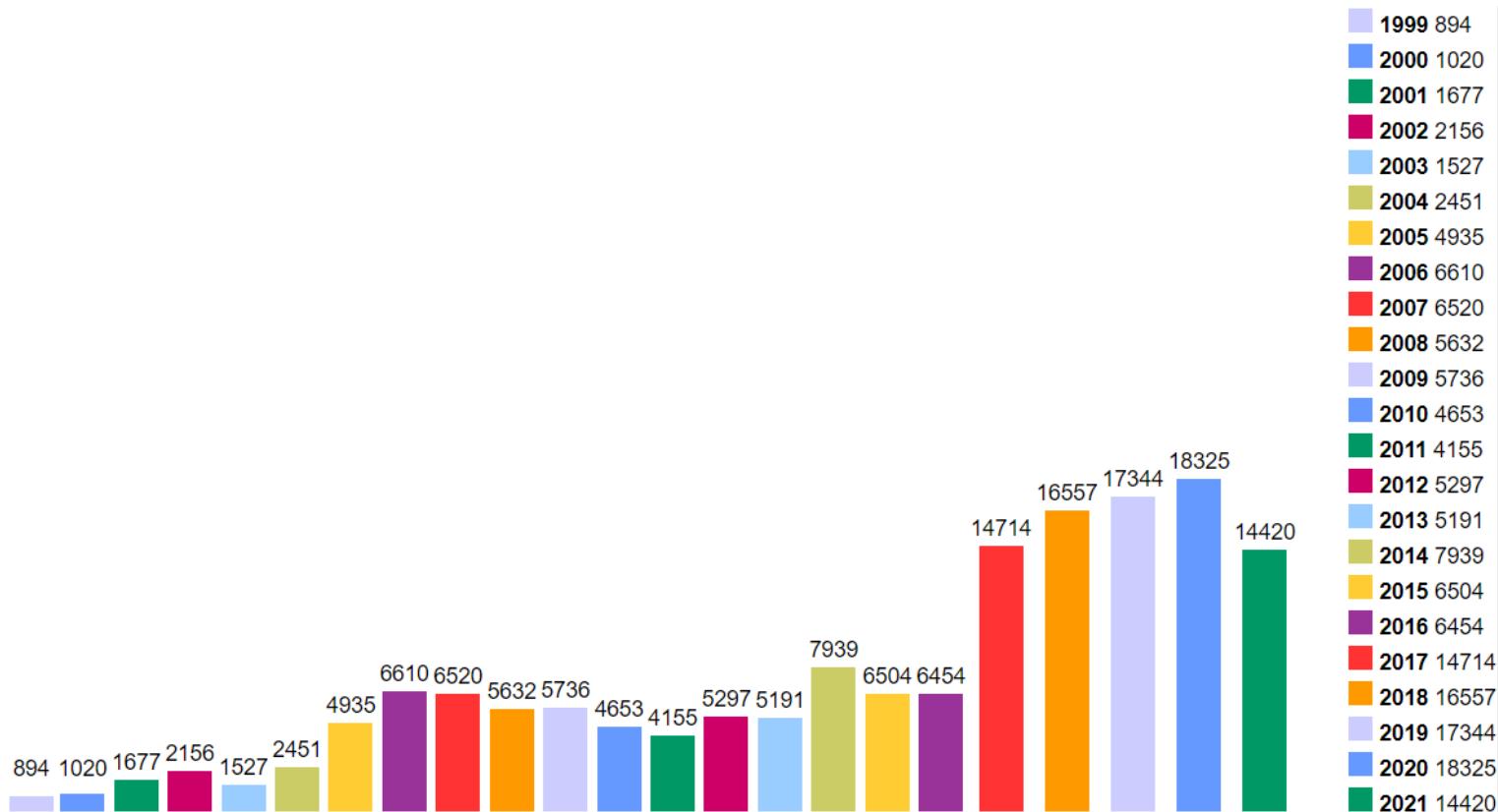
Checker & Exploit Code for CVE-2020-1472 aka Zerologon

Tests whether a domain controller is vulnerable to the Zerologon attack, if vulnerable, it will reset the Domain Controller's account password to an empty string.

NOTE: It will likely break things in production environments (eg. DNS functionality, communication with replication Domain Controllers, etc); target clients will then not be able to authenticate to the domain anymore, and they can only be re-synchronized through manual action. If you want to know more on how Zerologon attack break things, thanks to



# CVE por ano – cvedetails.com (as of Sep 2021)



# Ataques de dia Zero (0 day)

- **Ataque que usa vulnerabilidades que são**
  - Desconhecidas de terceiros
  - Não comunicadas ao fornecedor de software
- **Ocorre no dia zero do conhecimento dessas vulnerabilidades**
  - Para as quais não existe correção (ou não está aplicada)
- **Um ataque “0 day” pode existir por meses/anos**
  - Conhecido para atacantes mas não para utilizadores
  - Parte frequente de arsenais de ataques informáticos
  - Comercializados em mercados específicos

# ShadowBrokers

- **Background:** Atores estatais possuem arsenal para explorar vulnerabilidades desconhecidas do público
  - Parte integrante das suas atividades, por muitos anos e nunca reveladas
- **Agosto 2016:** Shadowbrokers publicam um grande quantidade de ferramentas deste atores
  - Usando canais públicos: Twitter, Github, PasteBin, Medium
  - Apresentam outras ferramentas: fazem um leilão, fazem uma venda de Black Friday, etc...
  - Objetivo: vender ferramentas que exploram 0 days a quem pagar mais
- **Março 2017:** Microsoft lança atualizações para várias versões de Windows
  - mas não lança para o W7, W8, XP e Server 2003
  - poderá ter existido dica de investigadores ou atores estatais
  - gravidade da atualização não é realçada

# ShadowBrokers

- **Abril 2017: ETERNALBLUE libertada ao público num dos pacotes**
  - Explora vulnerabilidade no MS Windows SMB v1 (Remote Code Execution)
- **Maio 2017: WannaCry ransomware**
  - Utiliza 2 exploits libertados pelos SB (ETERNALBLUE é o 1º)
  - Impacto: Cifra ficheiros, afeta > 300K dispositivos
  - Pede resgate de \$300-\$600 para obtenção da chave de decifra
- **Maio 2017: EternalRocks ransomware**
  - Utiliza 7 exploits libertados pelos SB (ETERNALBLUE é o 1º)
  - Impacto: Pânico apenas. Autor desativa ataque
- **Junho 2017: NotPetya ransomware**
  - Variante que utiliza ETERNALBLUE e cifra ficheiros
  - Pede resgate de \$300 (mas não é possível decifrar ficheiros)
  - Alvo: Infraestruturas críticas, bancos, jornais na Ucrânia e Rússia (outros tb afetados)
  - Impacto: Ficheiros perdidos, >\$10B de danos

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:  
`1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX`
2. Send your Bitcoin wallet ID and personal installation key to e-mail: `womsmith123456@posteo.net`. Your personal installation key:  
`X86GcZ-7PRNBE-3MNFMp-z88UnG-uF5nhF-4wzxwZ-XdNrr6-FYG89D-xk4rNz-9`



# Sobrevivência

**Como se sobrevive a uma ataque do dia zero?**

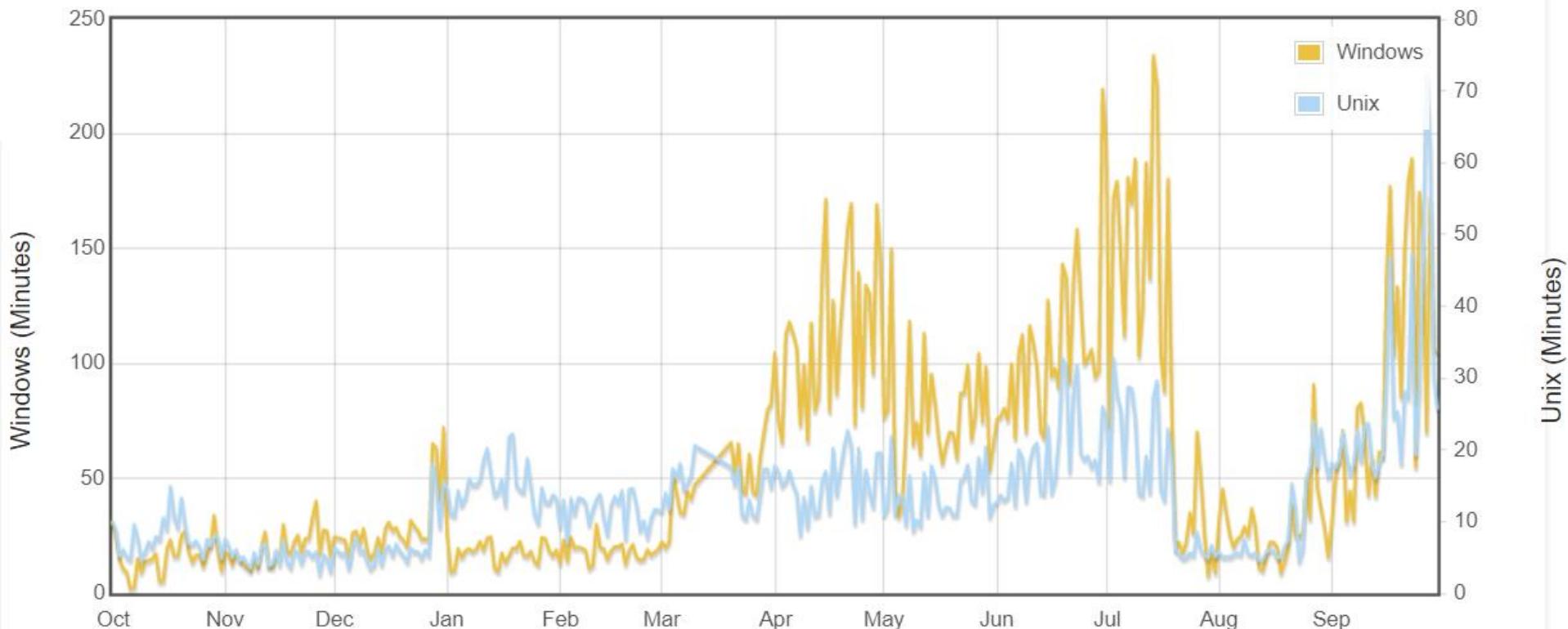
**Como se reage a uma ataque do dia zero massivo?**

- Diversidade poderá ser uma solução ...
  - Mas a produção, distribuição e atualização de software vai no sentido contrário!
    - E o mesmo acontece com as arquiteturas de hardware
  - Porque é que o MS Windows é um alvo primordial?
    - E o MAC OS nem por isso?
  - Está a usar um telemóvel Android?
    - Qual é a probabilidade de estar na linha da frente das vítimas?
    - iOS pode ser pior, pois o ecossistema é ainda mais homogéneo
- Coordenação é um grande auxílio

# Mean Survival Time

Oct 2020 – Oct 2021

(<http://isc.sans.org/survivaltime.html>)



- Um defensor tem de investir constantemente na segurança de um sistema
- Um atacante só necessita de ter sucesso uma vez em cada sistema
  - Atacantes podem tentar constantemente com ferramentas automáticas.

# CERT: Computer Emergency Readiness Team

- **Organização para garantir que as práticas de gestão de tecnologias e sistemas são usadas para:**
  - Resistir a ataques em sistemas distribuídos (em rede)
  - Limitar o dano, garantir a continuidade de serviços críticos
    - Mesmo considerando ataques realizados com sucesso, acidentes e falhas
- **CERT/CC (Coordination Center) @ CMU**
  - Um componente do CERT Program
  - Um hub para questões de segurança na Internet
    - Criado em Novembro 1988 depois do "Morris Worm"
    - Tem demonstrado a crescente exposição da Internet a ataques

# CSIRT: Computer Security Incident Response Team

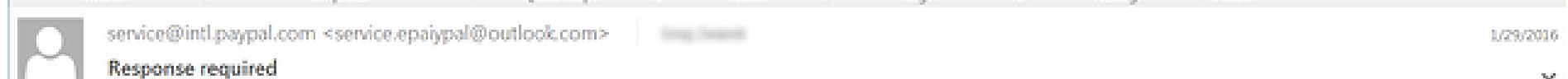
- **Organização responsável por receber, rever e responder a relatórios de incidentes e atividade**
  - Serviço 24/7 para usuários, companhia, agências governamentais e organizações
  - Ponto único de contato fiável e confiável para reportar incidentes de segurança à escala global
  - Meios para reportar incidentes e disseminar informação relativa a incidentes
- **CSIRTs Nacionais**
  - CERT.PT:
    - <https://www.facebook.com/CentroNacionalCibersegurancaPT>
  - National CSIRT Network
    - <https://www.redecsirt.pt>
  - CSIRT @ UA
    - <https://csirt.ua.pt>

# Alertas de segurança & tendências de atividades

- **Vitais para a disseminação rápida de conhecimento sobre novas vulnerabilidades**
  - US-CERT Technical Cyber Security Alerts
  - US-CERT (non-technical) Cyber Security Alerts
  - SANS Internet Storm Center
    - Aka DShield (Defense Shield)
  - Microsoft Security Response Center
  - Cisco Security Center
- E muitos outros

# Ataques Comuns: Phishing

- **Criam réplicas de páginas/serviços**
  - Imitam serviços fidedignos
  - URL tenta ser semelhante ao original
- **Link enviado para vítimas através de email/SMS**
  - Por vezes de computadores de colegas
    - Maior probabilidade da vítima confiar no serviço
- **Objetivo**
  - obter dados das vítimas
    - Senhas dos serviços
    - Números de cartões de crédito
  - obter dinheiro
  - levar vítima a instalar malware



 **Response required.**

Dear [REDACTED],

We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, [log in](#) to your account and go to the [Resolution Center](#).

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,  
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

# Ataques Comuns: Malware

- **Infetam sistemas com código malicioso**
  - **Vírus:** Necessitam de um hospedeiro (binário/documento)
  - **Worm:** Não necessita de um hospedeiro
  - **Trojan:** Disfarça-se de um programa benigno
- **Operação**
  - Vítima executa ficheiro infetado
    - Ou malware infeta sistema através de porto aberto
  - Vírus propaga-se para outros sistemas
    - Portos, documentos escritos, envio de emails
  - Malware pode tornar-se persistente
    - BIOS, Impressoras, outros suportes de armazenamento
  - Malware pode manter-se adormecido
    - Parte de uma infraestrutura de Comando e Controlo (C2)

# Ataques comuns: Ransomware

- Têm como objetivo obter um pagamento por parte da vítima
- Operação
  - Executam código malicioso num computador
  - Código compromete CIA
    - C: Envia informação para um servidor remoto
    - I: Apaga/corrompe/cifra informação
    - A: Cifra informação
  - Atacante exige pagamento para:
    - Não divulgação de informação
    - Recuperação de informação (fornece chave de decifra)
  - Ou atacante utiliza diretamente informação
    - Cartões VISA, credenciais de páginas



# Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37



Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37



## What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

## Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

## How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

GMT+5 (Moscow, Paris, Berlin)

[About bitcoin](#)

[How to buy bitcoins?](#)



Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

[Copy](#)

[Contact Us](#)

[Check Payment](#)

[Decrypt](#)

# Ataques comuns: keyloggers/spyware

- **Programa que regista eventos num sistema**
  - Teclas pressionadas
  - Capturas de ecrã
  - Imagens das webcam
- **Dados são enviados para sistema do atacante**
- **Objetivo:**
  - Extorsão (imagens capturadas)
  - Uso de informações obtidas
    - Passwords
    - Números de cartão de crédito

# Criptografia

# Terminologia

- **Criptografia**

- Arte ou ciência de escrever de forma escondida/confidencial
  - do Gr. kryptós, oculto + graph, r. de graphein, escrever
- Inicialmente para garantir a privacidade da informação
- Esteganografia
  - do Gr. steganós, oculto + graph, r. de graphein, escrever

- **Criptanálise**

- Arte ou ciência de quebrar sistemas criptográficos ou informação criptografada

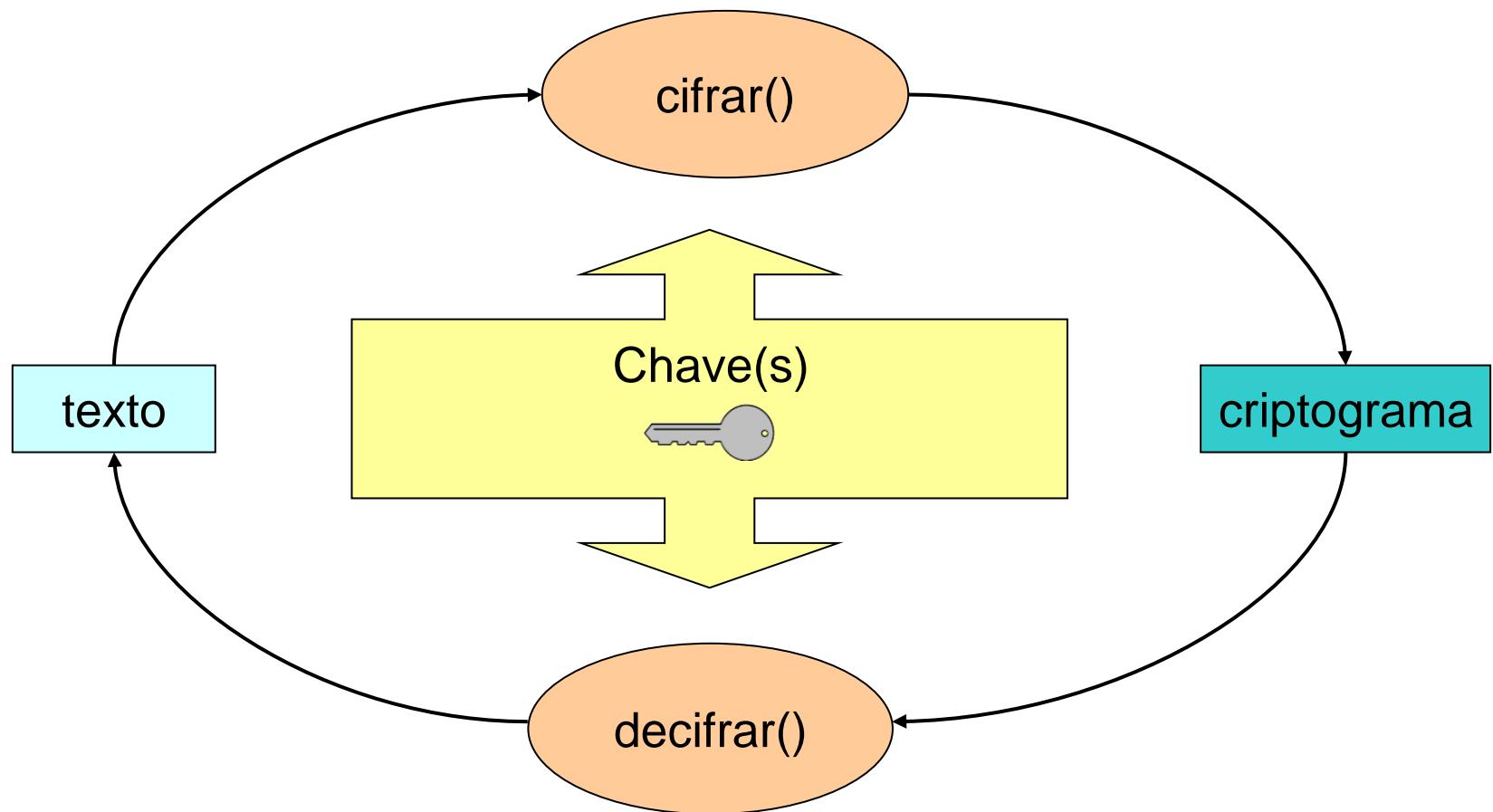
- **Criptologia**

- Criptografia + criptanálise

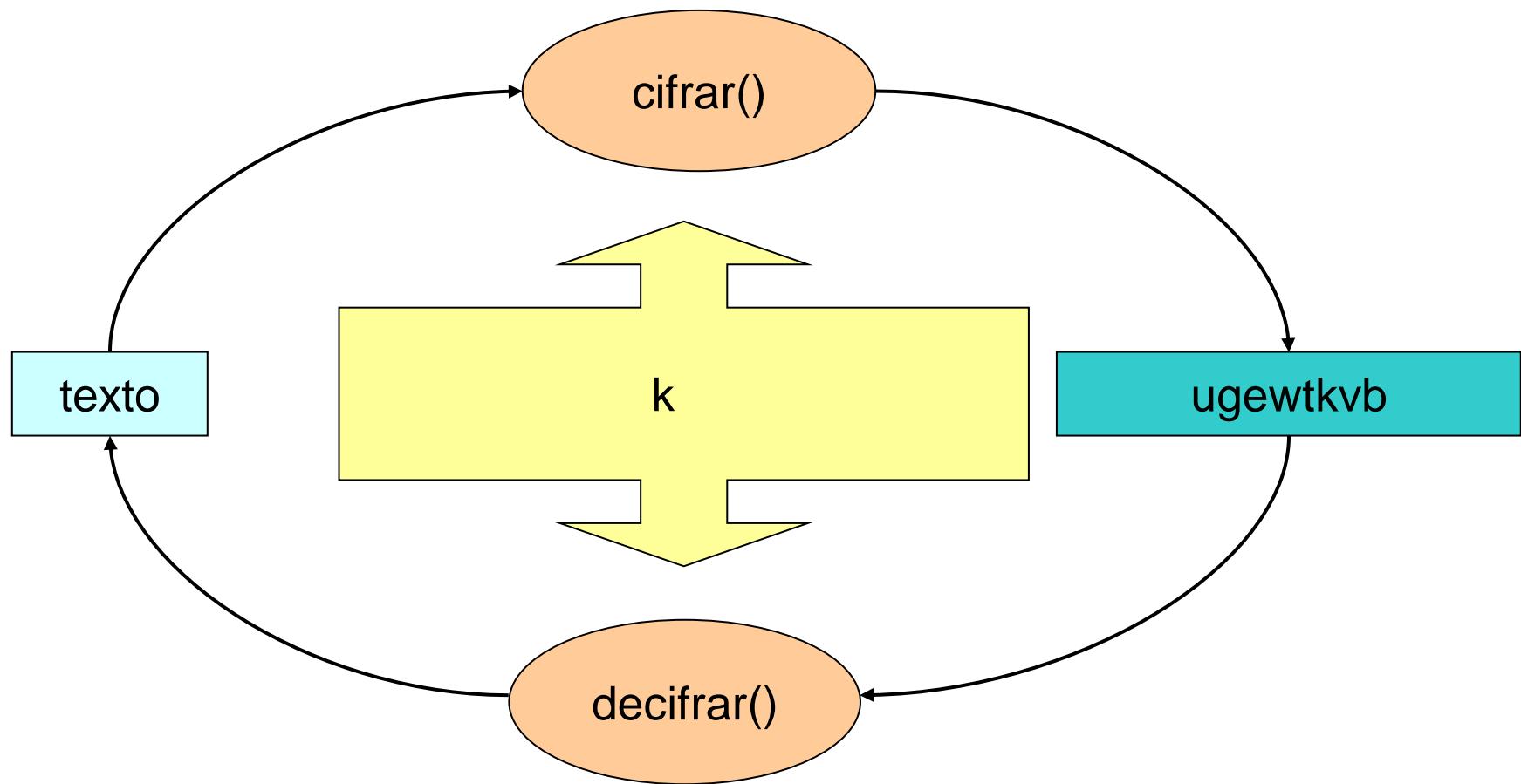
# Terminologia

- **Cifra**
  - Técnica concreta de criptografia
- **Operação de uma cifra**
  - **Cifra:** texto em claro -> criptograma
  - **Decifra:** criptograma -> texto em claro
- **Algoritmo:** modo de transformação de dados
- **Chave:** parâmetro do algoritmo
  - Influencia a operação do algoritmo

# Operações de uma cifra



# Operações de uma cifra



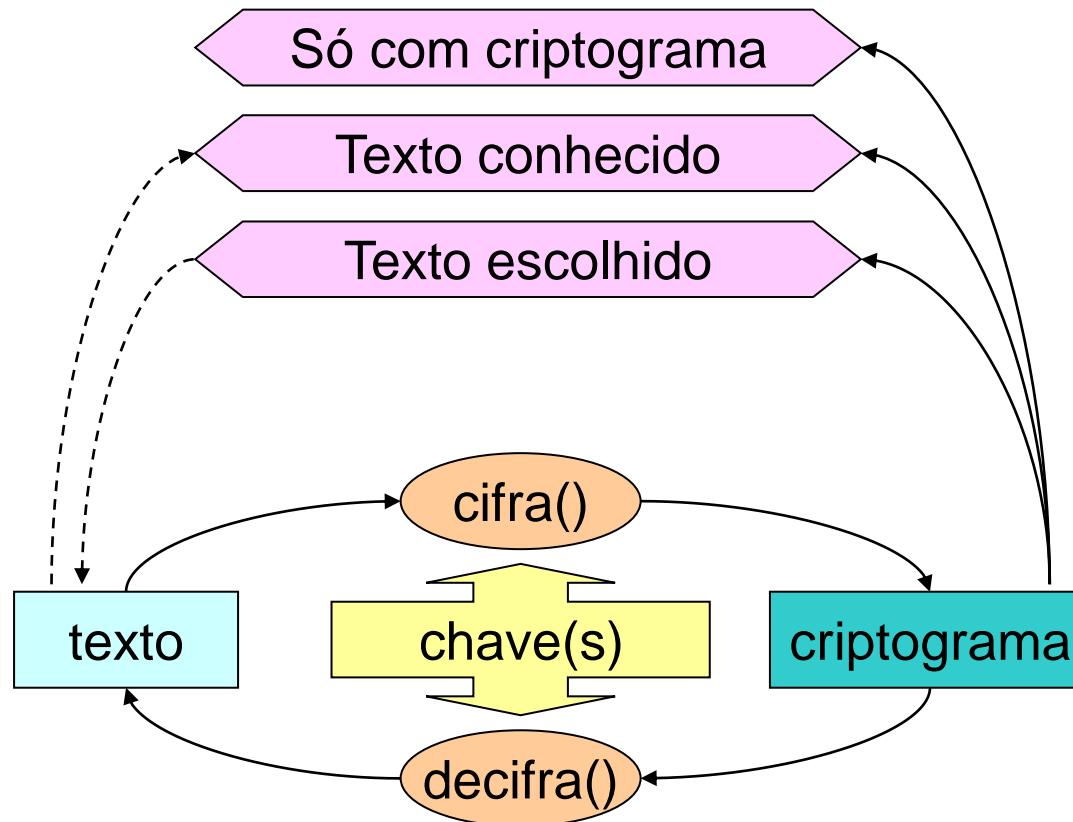
# Casos de uso (Cifras Simétricas)

- **Proteção própria com chave K**
  - Alice cifra texto P com chave K  
-> Alice:  $C = \{P\}_k$
  - Alice decifra C com chave K  
-> Alice:  $P' = \{C\}_k$
  - $P'$  deverá ser igual a P (deve ser verificado)
- **Comunicações seguras com chave K**
  - Alice cifra texto P com chave K  
-> Alice:  $C = \{P\}_k$
  - Bob decifra C com chave K  
-> Bob:  $P' = \{C\}_k$
  - $P'$  deve ser igual a P (deve ser verificado)

# Criptanálise: Objetivos

- **Obtenção do texto original**
  - Relativo a um criptograma
- **Obtenção de uma chave de cifra**
  - Ou de uma equivalente
- **Obtenção do algoritmo de cifra**
  - Ou de um equivalente
  - Normalmente os algoritmos não são secretos, mas existem exceções:
    - Lorenz, A5 (GSM), RC4, Crypto-1 (Mifare)
    - Algoritmos para DRM (Digital Rights Management)
  - Por engenharia reversa

# Ataques por Criptanálise



# Ataques por Criptanálise

- **Força Bruta (ataque genérico)**
  - Pesquisa exaustiva sobre todo o espaço de chaves, até se encontrar uma chave adequada
  - Não é prática para espaços de dimensão grande
    - ex. chaves de 128 bits possuem um espaço de  $2^{128}$  bits.
  - É importante que exista aleatoriedade na chave.
- **Ataques mais inteligentes**
  - Reduzir o espaço de pesquisa para uma dimensão menor:: palavras, números, conjunto reduzido, alfabeto
  - Identificar padrões em algumas operações, etc..

# Evolução das Cifras

- **Manuais:** Algoritmos de substituição ou transposição



Fonte: Wikimedia Commons e CryptoMuseum

# Evolução das Cifras

- **Mecânicas**

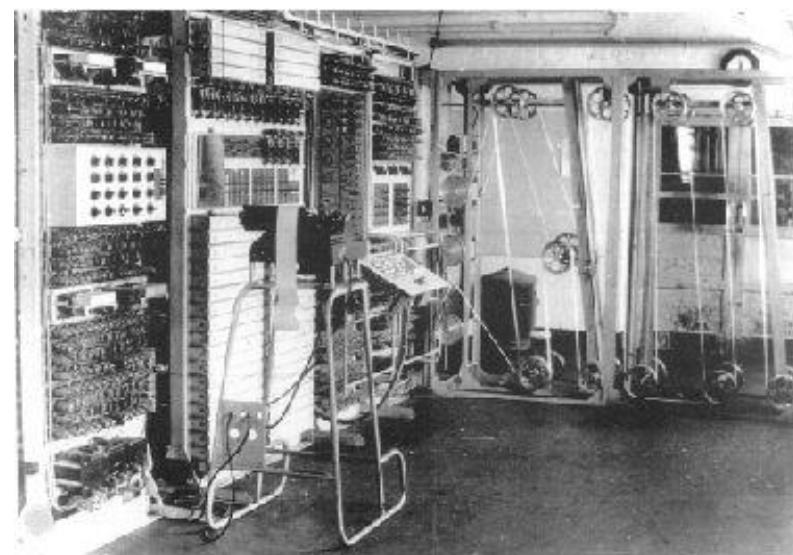
- A partir do Séc. XIX
  - Máquina Enigma
  - M-209 Converter
- Algoritmos de substituição ou transposição
  - Elementos críticos para a 2ª Grande Guerra



# Evolução das Cifras

- **Cifras Informáticas**

- Surgem com o uso dos computadores
- Algoritmos de substituição mais complexos
- Algoritmos matemáticos de grandes números ou problemas complexos
- Utilizados de forma comum (e transparente) no dia a dia



# Cifras: Tipos Básicos

- **Transposição:** O texto original é “baralhado”

O	O	I	B	H
T	O	N	A	A
E	R	A	R	D
X	I	L	A	O
T	G	E	L	

- **Resultado:** ooibh tonaa erard xilao tgel

# Cifras: Tipos Básicos

- **Transposição:** Permutações intra-blocos

P	E	R	M	U
T	A	C	O	E
S	I	N	T	R
A	B	L	O	C
O	S			

- **Resultado:**
  - (13524) -> pruem tceao snrit alcbo os
  - (25413) -> eumpr aeotc irtsn bcoal so

# Cifras: Tipos Básicos

- **Substituição**
  - Cada símbolo original é substituído por outros
  - Considera símbolos como letras, dígitos e pontuação
  - Na realidade são blocos de bits
- **Estratégias de substituição**
  - Mono alfabética (um para um)
  - Poli-alfabética (muitos para um)
  - Homofônica (um para muitos)

# Cifras: Mono-alfabéticas

- **Usam apenas um alfabeto de substituição**
  - Com um número de elementos #A
- **Exemplos**
  - Aditivas (ou de translação)
    - cripto - letra = (letra + chave) mod #A
    - letra = (cripto - letra – chave) mod #A
    - Número de chaves efetivas = #A
    - Cifra de César (ROT-x)
  - Com frase-chave
    - ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - QTUWXYZCOMFRASEHVBBDGJKLNP
    - Número de chaves efetivas = #alfabeto! ->  $26! \approx 288$
- **Problemas**
  - Reproduzem padrões do texto original
  - Letras, digramas, trigramas, etc.
  - A análise estatística facilita a criptanálise
  - “The Gold Bug”, Edgar Alan Poe

# Cifras: Mono-alfabéticas

a good glass in the  
bishop's hostel in the  
devil's seat fifty-one  
degrees and thirteen  
minutes northeast and  
by north main branch  
seventh limb east side  
shoot from the left eye  
of the death's-head a  
bee line from the tree  
through the shot forty  
feet out

53‡††305))6\*;4826)4‡.)  
4‡);806\*;48†860))85;1‡  
(;:‡\*8†83(88)5\*†;46(;8  
8\*96\*?;8)\*†(;485);5\*†2  
:\*‡(;4956\*2(5\*—4)88\*;4  
069285);)6†8)4‡‡;1(‡9;  
48081;8:8‡1;48†85;4)48  
5†528806\*81(‡9;48;(88;  
4(‡?34;48)4‡;161;:188;  
‡?;

# Cifras: Mono-alfabéticas

53‡‡305))6\*;4826)4‡.)4‡);80  
agooodglassinthebishophostel

6\*;48†8¶60))85;1‡(;‡\*8†83(88)  
inthedevilsseatfortyonedegrees

5\*t;46(;88\*96\*?;8)\*‡(;485);5\*t  
andthirteenminutesnortheastand

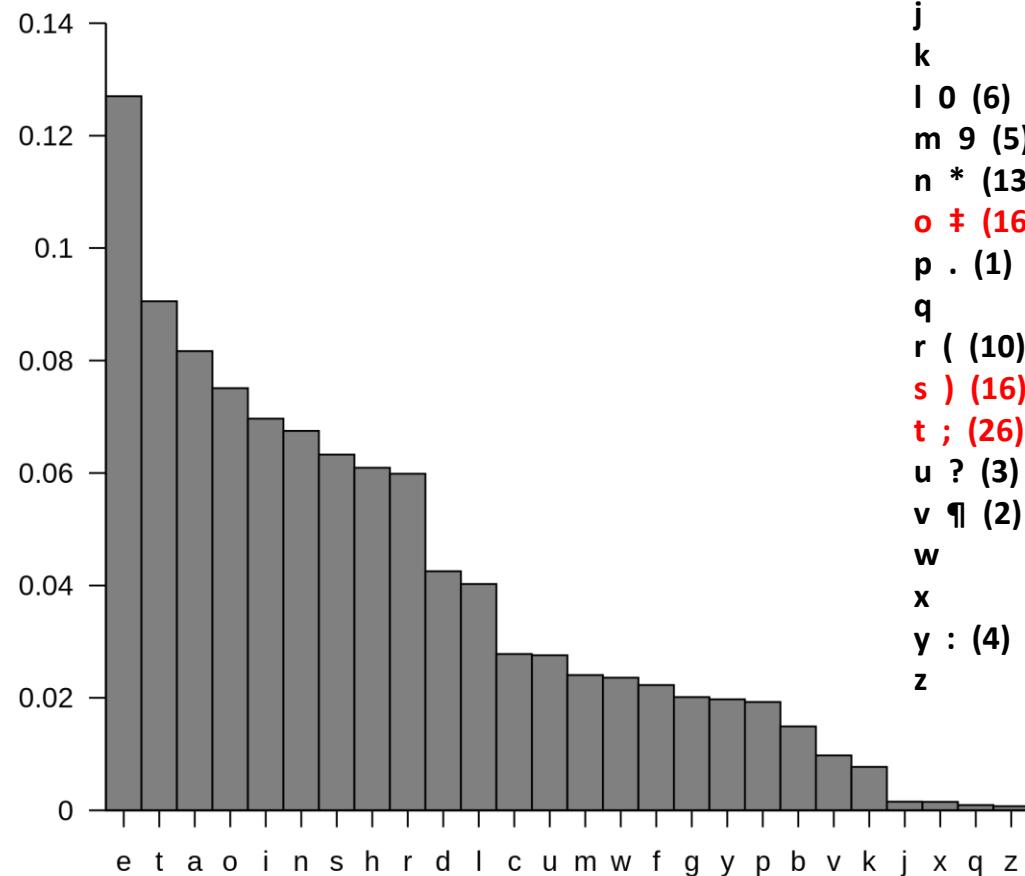
2:\*‡(;4956\*2(5\*-4)8¶8\*;40692  
bynorthmainbranchseventhlimb

85);)6†8)4‡‡;1(‡9;48081;8:8‡1  
eastsideshootfromthelefteyeof

;48†85;4)485†528806\*81(‡9;48  
thedeathsheadabeelinefromthe

;(88;4(‡?34;48)4‡;161;:188;‡?;  
treethroughtheshotfiftyfeetout

a	5	(12)
b	2	(5)
c	-	(1)
d	†	(8)
e	8	(33)
f	1	(8)
g	3	(4)
h	4	(19)
i	6	(11)
j		
k		
l	0	(6)
m	9	(5)
n	*	(13)
o	‡	(16)
p	.	(1)
q		
r	(	(10)
s	)	(16)
t	;	(26)
u	?	(3)
v	¶	(2)
w		
x		
y	:	(4)
z		



# Cifras: Mono-alfabéticas

- **Frequência de Pares**
  - AO, NO, AS, OS, SO, UM, IA, NA...
- **Frequência de Triplos**
  - QUE, NAO, EST, ENT, ÇÃO, TRA...
- **Probabilidades condicionais**
  - $P(A | B)$  diferente de  $P(Z | B)$

# Cifras: Poli-alfabéticas

- Usam **N** alfabetos de substituição
  - Têm período **N**
- Exemplo: Cifra de Vigenère
- Problemas
  - Conhecido o período, podem ser analisadas como N mono alfabéticas
    - O período pode ser descoberto usando estatística
  - Método de Kasiski
    - Fatorização de distâncias entre blocos iguais do criptograma
  - Índice de coincidência
    - Fatorização de deslocamentos relativos que produzem mais coincidências na sobreposição do criptograma

# Cifra de Vigenère

	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
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Exemplo de se cifrar a letra **M** com a chave **S**, resultando no criptograma **E**

Criada por Blaise Vigenère (final séc XVI) (le chiffre indéchiffrable!)

Quebrada no séc XIX por Charles Babbage e Friedrich Kasiski

# Cifra de Vigenère

- **Texto:**

Eles não sabem que o sonho é uma constante da vida  
tão concreta e definida como outra coisa qualquer,  
como esta pedra cinzenta em que me sento e descanso,  
como este ribeiro manso, em serenos sobressaltos  
como estes pinheiros altos
  - **Cifra com o quadrado de Vigenère e chave “poema”**

**texto**      **elesnaosabemqueesonhoeumaconstantedavidaconcretae definida**

**criptograma** tzienpcwmbtaugedgszhdsyyarcretpbxqdpjmpaiosoocqvqtpshqfxbmpa

# Criptanálise de um criptograma Vigenère

## Teste de Kasiski

- Localizar padrões comuns no criptograma
- Calcular afastamento entre padrões
- O maior divisor comum sugere a dimensão da chave (gcd)

tziencwmbtaugedgszhdsyyarcretpbxqdpjmpaosooocqvqtphqfxbmpa

mpa	$20 = 2 \times 2 \times 5$
tp	$20 = 2 \times 2 \times 5$

- Com o texto indicado:

$$\begin{aligned}175 &= 5 \times 5 \times 7 \\105 &= 3 \times 5 \times 7 \\35 &= 5 \times 7 \\20 &= 2 \times 2 \times 5\end{aligned}$$

- Com o poema completo:

# Criptanálise de um criptograma Vigenère

- Índice de coincidência (c/ poema completo)
  - Sobreposição de uma cópia, com afastamento
  - Contagem dos caracteres que se repetem

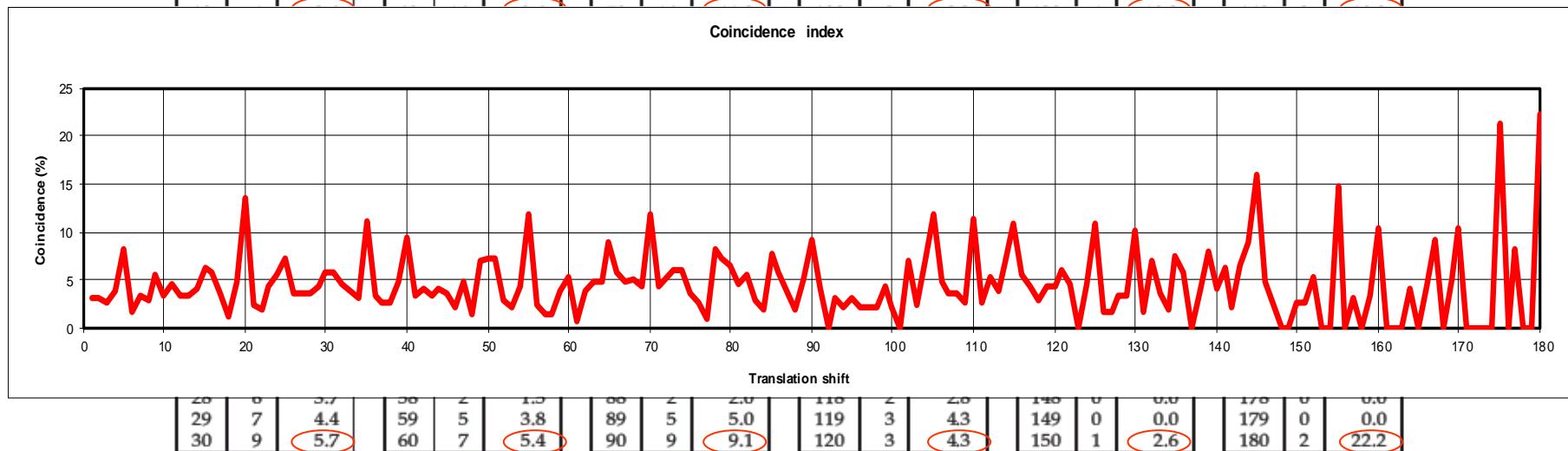
D	I	P (%)	D	I	P (%)	D	I	P (%)	D	I	P (%)	D	I	P (%)	D	I	P (%)
1	6	3.2	31	9	5.7	61	1	0.8	91	4	4.1	121	4	5.9	151	1	2.6
2	6	3.2	32	7	4.5	62	5	3.9	92	0	0.0	122	3	4.5	152	2	5.4
3	5	2.7	33	6	3.8	63	6	4.8	93	3	3.1	123	0	0.0	153	0	0.0
4	7	3.8	34	5	3.2	64	6	4.8	94	2	2.1	124	3	4.6	154	0	0.0
5	15	8.2	35	17	11.0	65	11	8.9	95	3	3.2	125	7	10.9	155	5	14.7
6	3	1.6	36	5	3.3	66	7	5.7	96	2	2.2	126	1	1.6	156	0	0.0
7	6	3.3	37	4	2.6	67	6	4.9	97	2	2.2	127	1	1.6	157	1	3.1
8	5	2.8	38	4	2.6	68	6	5.0	98	2	2.2	128	2	3.3	158	0	0.0
9	10	5.6	39	7	4.7	69	5	4.2	99	4	4.4	129	2	3.3	159	1	3.3
10	6	3.4	40	14	9.4	70	14	11.8	100	2	2.2	130	6	10.2	160	3	10.3
11	8	4.5	41	5	3.4	71	5	4.2	101	0	0.0	131	1	1.7	161	0	0.0
12	6	3.4	42	6	4.1	72	6	5.1	102	6	6.9	132	4	7.0	162	0	0.0
13	6	3.4	43	5	3.4	73	7	6.0	103	2	2.3	133	2	3.6	163	0	0.0
14	7	4.0	44	6	4.1	74	7	6.1	104	6	7.1	134	1	1.8	164	1	4.0
15	11	6.3	45	5	3.5	75	4	3.5	105	10	11.9	135	4	7.4	165	0	0.0
16	10	5.8	46	3	2.1	76	3	2.7	106	4	4.8	136	3	5.7	166	1	4.3
17	6	3.5	47	7	4.9	77	1	0.9	107	3	3.7	137	0	0.0	167	2	9.1
18	2	1.2	48	2	1.4	78	9	8.1	108	3	3.7	138	2	3.9	168	0	0.0
19	8	4.7	49	10	7.1	79	8	7.3	109	2	2.5	139	4	8.0	169	1	5.0
20	23	13.6	50	10	7.2	80	7	6.4	110	9	11.4	140	2	4.1	170	2	10.5
21	4	2.4	51	10	7.2	81	5	4.6	111	2	2.6	141	3	6.2	171	0	0.0
22	3	1.8	52	4	2.9	82	6	5.6	112	4	5.2	142	1	2.1	172	0	0.0
23	7	4.2	53	3	2.2	83	3	2.8	113	3	3.9	143	3	6.5	173	0	0.0
24	9	5.5	54	6	4.4	84	2	1.9	114	5	6.7	144	4	8.9	174	0	0.0
25	12	7.3	55	16	11.9	85	8	7.7	115	8	10.8	145	7	15.9	175	3	21.4
26	6	3.7	56	3	2.3	86	6	5.8	116	4	5.5	146	2	4.7	176	0	0.0
27	6	3.7	57	2	1.5	87	4	3.9	117	3	4.2	147	1	2.4	177	1	8.3
28	6	3.7	58	2	1.5	88	2	2.0	118	2	2.8	148	0	0.0	178	0	0.0
29	7	4.4	59	5	3.8	89	5	5.0	119	3	4.3	149	0	0.0	179	0	0.0
30	9	5.7	60	7	5.4	90	9	9.1	120	3	4.3	150	1	2.6	180	2	22.2

# Criptanálise de um criptograma Vigenère

- Índice de coincidência (c/ poema completo)
  - Sobreposição de uma cópia, com afastamento
  - Contagem dos caracteres que se repetem

D	I	P (%)
1	6	3.2
2	6	3.2
3	5	2.7
4	7	3.8
5	15	8.2
6	3	1.6
7	6	3.3
8	5	2.8
9	10	5.6
31	9	5.7
32	7	4.5
33	6	3.8
34	5	3.2
35	17	11.0
36	5	3.3
37	4	2.6
38	4	2.6
39	7	4.7
61	1	0.8
62	5	3.9
63	6	4.8
64	6	4.8
65	11	8.9
66	7	5.7
67	6	4.9
68	6	5.0
69	5	4.2
91	4	4.1
92	0	0.0
93	3	3.1
94	2	2.1
95	3	3.2
96	2	2.2
97	2	2.2
98	2	2.2
99	4	4.4
121	4	5.9
122	3	4.5
123	0	0.0
124	3	4.6
125	7	10.9
126	1	1.6
127	1	1.6
128	2	3.3
129	2	3.3
151	1	2.6
152	2	5.4
153	0	0.0
154	0	0.0
155	5	14.7
156	0	0.0
157	1	3.1
158	0	0.0
159	1	3.3

Coincidence index



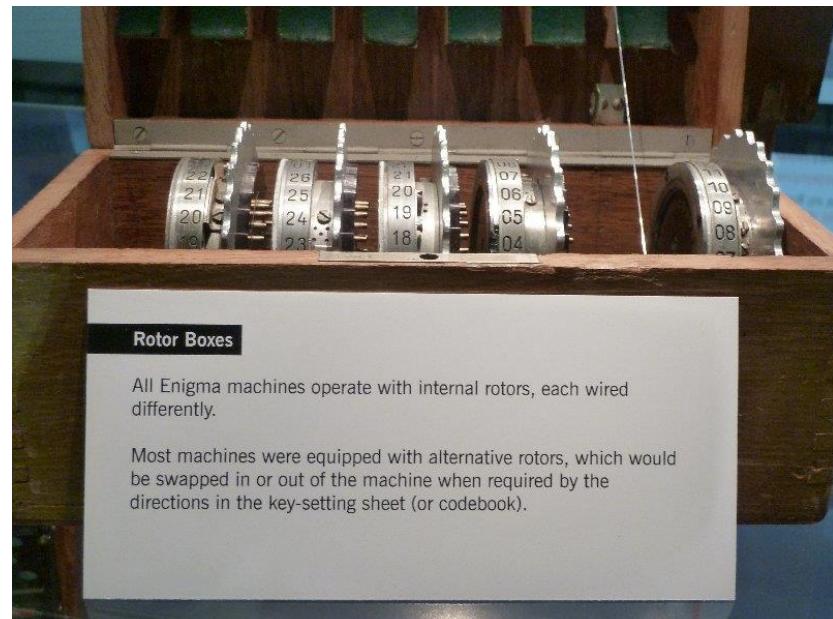
28	0	5.7
29	7	4.4
30	9	5.7
58	5	3.8
59	5	3.8
60	7	5.4
88	5	5.0
89	9	9.1
118	3	4.3
119	3	4.3
120	3	4.3
148	0	0.0
149	1	2.6
150	2	22.2
178	0	0.0
179	0	0.0
180	2	22.2

# Máquinas de Rotores



# Máquinas de Rotores

- As máquinas de rotore concretizam cífras poli-alfabéticas complexas
  - Cada rotor efetua uma permutação do alfabeto
    - Que consiste num conjunto de substituições
  - A posição do rotor concretiza um alfabeto de substituição
  - A rotação de um rotor concretiza uma cifra poli-alfabética
  - Acumulando vários rotore em sequência e rodando-os de forma diferenciada consegue-se uma cifra poli-alfabética complexa
- A chave de cifra é:
  - O conjunto de rotore usado
  - A ordem relativa dos rotore
  - A posição de avanço do rotor seguinte
  - A posição original dos rotore
- Rotore simétricos (bidirecionais) permitem decifrar usando cífras duplas
  - Usando um disco refletor (meio-rotor)

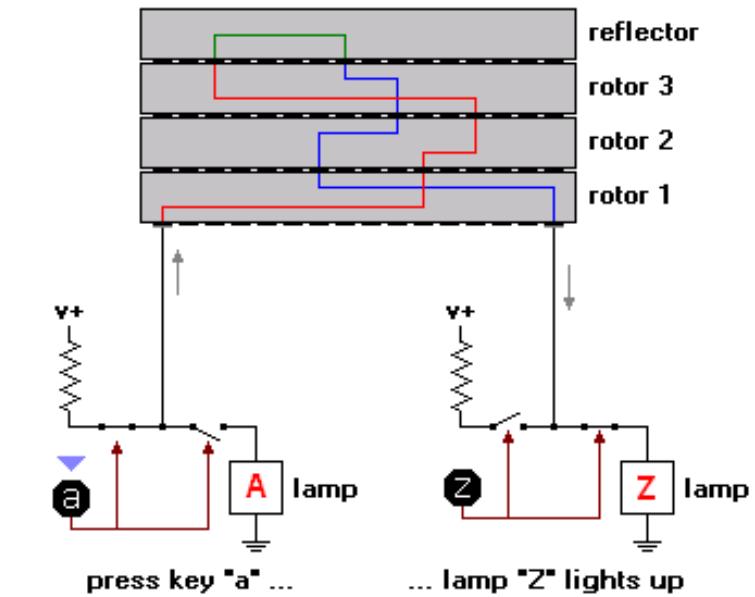


Sarah Witherby, [www.flickr.com](https://www.flickr.com)

# Máquinas de Rotores

- **Operação recíproca com um refletor**

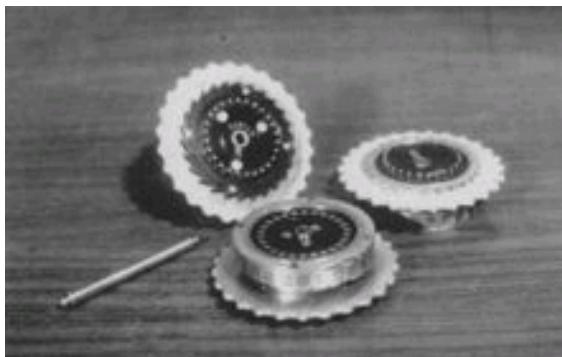
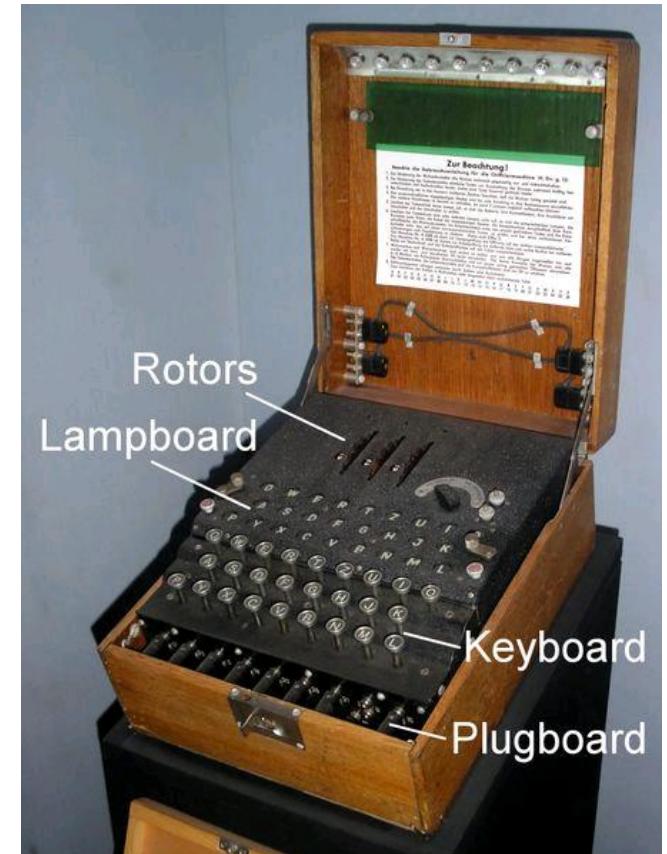
- O operador emissor carrega em “A” (o texto em claro) e obtém “Z” como criptograma, o qual é transmitido
- O operador receptor carrega em “Z” (o criptograma) e obtém “A” como texto em claro
- Uma letra nunca pode ser cifrada para si própria!



RECIPROCAL OPERATION OF THE ENIGMA

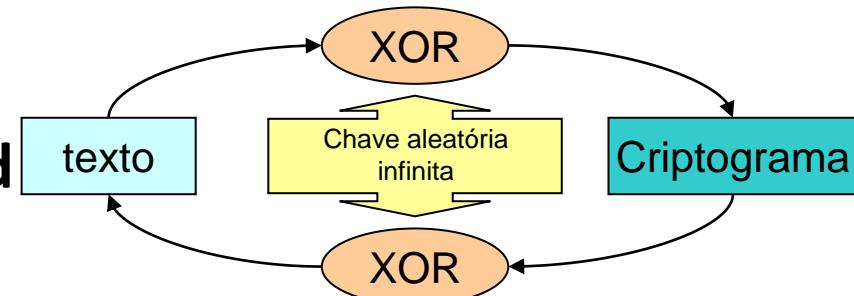
# Enigma

- Máquina de rotores alemã da 2<sup>a</sup> GG
- Originalmente apresentada em 1919
  - Enigma I, com 3 rotores
- Foram usadas diversas variantes
  - Com diferentes números de rotores
  - Com cablagem para permutar alfabetos
- Seleções de chaves distribuídas em livros de códigos
- <https://observablehq.com/@tmcw/enigma-machine>



# Criptografia: Aproximações Teóricas

- **Espaço de texto**
  - Número de combinações de texto diferentes ( $M$ )
- **Espaço do criptograma**
  - Número de combinações de criptograma diferentes ( $C$ )
- **Espaço das chaves**
  - Número de chaves diferentes para um algoritmo de cifra ( $K$ )
- **Cifra perfeita**
  - Dado  $c_j \in C$ ,  $H(M | C) = H(M)$ 
    - $H(M | C)$  é a entropia condicional de  $M$  dado  $C$
    - $H(M)$  é a entropia de  $M$
  - $\#K \geq \#C \geq \#M$
- **Cifra de Vernam: One-time pad**



# Criptografia: Aproximações Práticas

- **Teoricamente seguras vs. seguras na prática**
  - Uso teórico != exploração prática
  - Práticas incorretas podem comprometer boas cifras
  - Exemplo: reutilização de one-time-pads
- **Cifras seguras na prática**
  - A segurança é assegurada pela dificuldade computacional de realizar a criptanálise
    - Usando força bruta
  - Têm uma segurança baseada em limites razoáveis:
    - Custo de uma solução técnica de criptanálise
    - Infraestrutura reservada para a criptanálise
    - Tempo útil de criptanálise

# Criptografia: Aproximações Práticas

## 5 critérios de Shannon

### 1. A quantidade de secretismo oferecida

- e.g o comprimento da chave

### 2. A complexidade na escolha das chaves

- e.g. geração da chave, deteção de chaves fracas

### 3. A simplicidade da realização

### 4. A propagação de erros

- Relevante em ambientes com erros (canais de comunicação ruidosos)

### 5. A dimensão do criptograma

- Relativamente aos respetivos textos originais

# Criptografia: Aproximações Práticas

- **Confusão: Complexidade na relação entre o texto, a chave e o criptograma**
  - Os bits resultantes (criptograma) devem depender dos bits de entrada (texto e chave) de um forma complexa
- **Difusão: Alteração de **grandes porções** do criptograma em função de uma pequena alteração do texto**
  - Se um bit de texto se alterar, então o criptograma deverá **mudar substancialmente**, de uma forma imprevisível e pseudoaleatória
  - **Efeito de avalanche**

# Criptografia: Aproximações Práticas

## Assumir sempre o pior caso

- **O criptanalista conhece o algoritmo**
  - A segurança está na chave
- **O criptanalista possui grande número de criptogramas gerados com um algoritmo e chave**
  - Os criptogramas não são secretos
- **Os criptanalista conhecem parte dos textos originais**
  - É normal haver alguma noção do texto original
  - Ataques com texto conhecido
  - Ataques com texto escolhido

# Robustez criptográfica

- **A robustez dos algoritmos e a sua resistência a ataques**
  - Ninguém consegue avaliar a robustez de forma precisa
    - Podem especular ou demonstrar usando outras suposições
  - São robustos até que alguém os quebre
  - Existem orientações públicas sobre o que deve/não deve ser usado
    - Antecipar problemas futuros
- **Algoritmos públicos, sem ataques conhecidos, supostamente são mais robustos**
  - Mais investigadores à procura de fraquezas
- **Algoritmos com chaves maiores são tendencialmente mais robustos**
  - Mas frequentemente também são mais lentos.

# Robustez criptográfica: AES

- **1997: NIST lançou desafio para o próximo Advanced Encryption Protocol**
  - de conhecimento e utilização públicos, simétrico, chaves de 128, 192 e 256 bits
- **1998: 15 candidatos apresentados por investigadores**
  - CAST-256, Crypton, DEAL, DFC, Frog, HPC, LOKI97, Magenta, MARS, RC6, Rijndael, Safer+, Serpent, Twofish
  - Comunidade tentou encontrar problemas nos candidatos
- **1999: 5 propostas demonstraram ser seguras**
  - MARS, RC6, Rijndael, Twofish
  - Novamente a comunidade tentou encontrar problemas e avaliar a performance
- **2001: Rijndael selecionado como o vencedor**
  - Versões reduzidas do MARS foram quebradas , RC6 e Twofish são seguros
- **2002: Publicado como FIPS PUB 197 e é largamente utilizado**

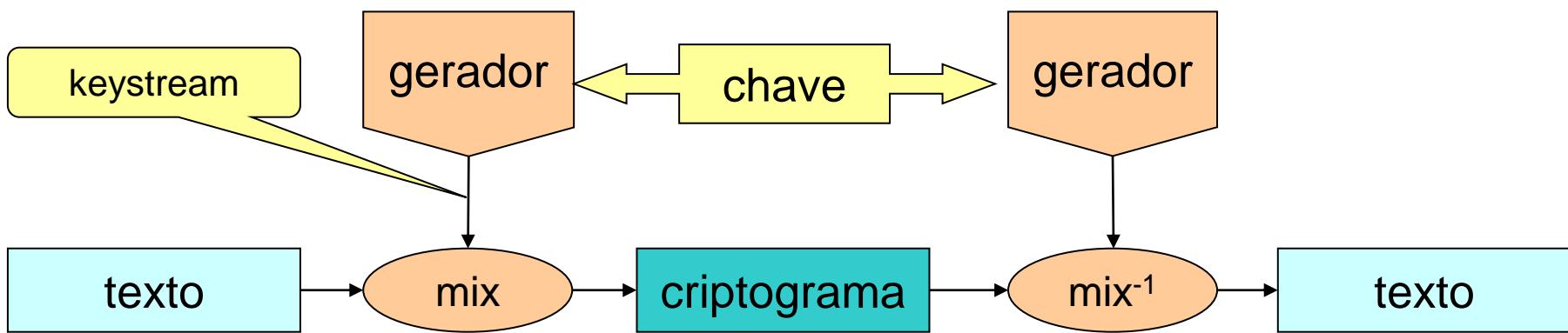
# Cifras Contínuas (Stream)

- Mistura de uma chave contínua (keystream) com o texto ou criptograma
  - Chave contínua aleatória (cifra de Vernam, one-time pad)
  - Chave contínua pseudoaleatória (produzida por gerador)
- Função de mistura invertível
  - e.g. XOR bit a bit ( $\oplus$ )

$$C = P \oplus ks \quad P = C \oplus ks$$

- Cifra poli-alfabética
  - Cada símbolo da chave contínua define um alfabeto

# Cifras Contínuas (Stream)



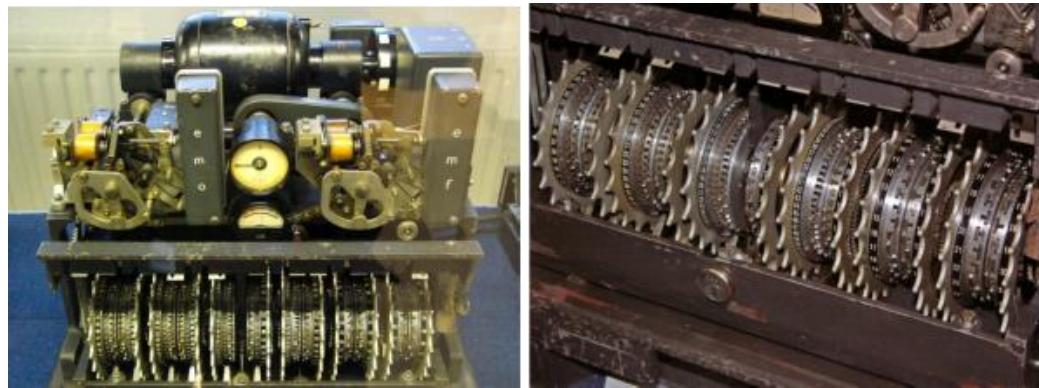
# Cifras Contínuas (Stream)

- Keystream pode ser infinita, mas possui um período
  - Período depende do gerador
- Questões práticas de segurança
  - Cada keystream só pode ser usada uma vez!
  - Caso contrário, a soma dos criptogramas fornece a soma dos textos

$$C_1 = P_1 \oplus K_s, \quad C_2 = P_2 \oplus K_s \quad \rightarrow \quad C_1 \oplus C_2 = P_1 \oplus P_2$$

- Dimensão do texto tem de ser menor que o período
  - Exposição da keystream é total com textos escolhidos/conhecidos
  - Período permitem analistas conhecer partes do texto
- Controlo de integridade é mandatório
  - Não existe difusão, apenas confusão
  - Criptogramas podem ser manipulados livremente

# Lorenz (Tunny)

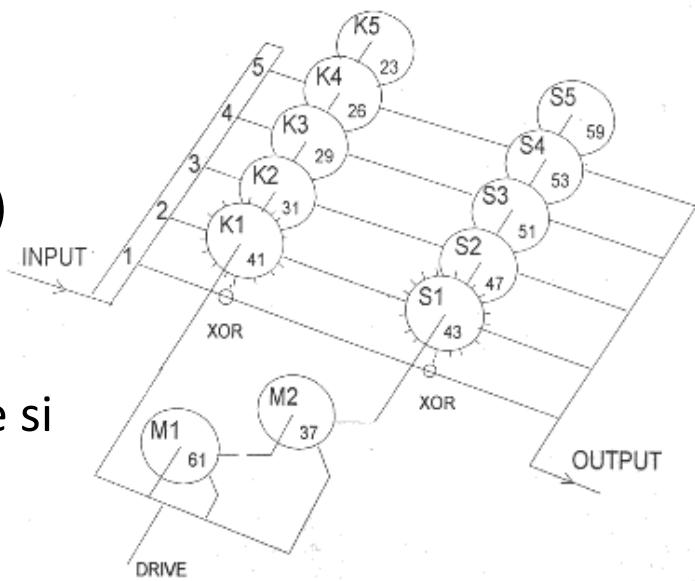


- **Cifra contínua com 12 rotores**

- Usada pelos alemães durante a 2 G. Guerra
- Cada caractere de 5 bits é misturado com 5 keystreams

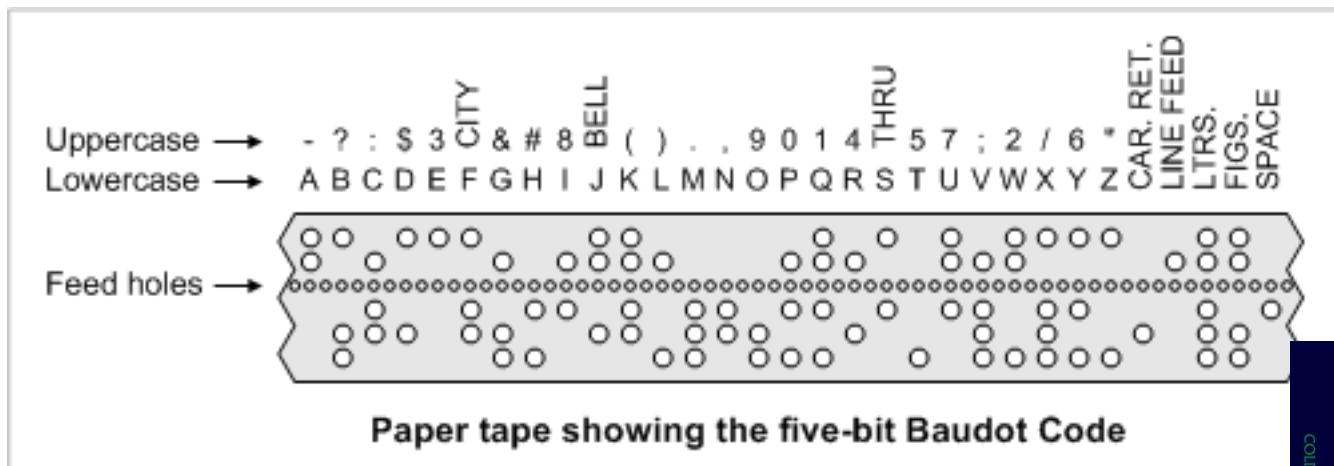
- **Operação**

- 5 rotores movendo-se regularmente ( $\chi$ )
- 5 rotores movendo-se irregularmente ( $\psi$ )
- 2 rotores motorizados
  - para acionar os rotores ( $\psi$ )
- Número de espaços é sempre primo entre si



# Criptanálise da Tunny

- A estrutura interna não era conhecida
  - Apenas foi conhecida depois do final da guerra
  - Sabiam que a máquina existia porque intercetavam mensagens cifradas com 5 bits
    - Usando Códigos Baudot de 32 símbolos (e não Morse)



De interesse: 2014, The Imitation Game



# Criptanálise da Tunny

## O erro (30 de agosto de 1941)

- Um operador alemão tinha uma grande mensagem para enviar (~4,000 caracteres)
  - Configurou a sua Lorenz e enviou um indicador de 12 letras (posição inicial dos rotores) para o receptor
  - Depois de ter escrito ~4,000 caracteres, manualmente, recebeu do receptor “envie outra vez” (em texto)
- O operador emissor recolocou a sua Lorenz na mesma posição inicial
  - Mesma chave contínua! Completamente proibido!
- O emissor recomeçou o envio da mensagem, manualmente
  - Mas escreveu algo ligeiramente diferente! (abreviaturas)

# Criptanálise da Tunny

$$C_0 = \text{Texto}_0 \oplus K_s$$

$$C_1 = \text{Texto}_1 \oplus K_s$$

$$T_1 = C_0 \oplus C_1 \oplus T_0 \rightarrow \text{Variações do Texto}$$

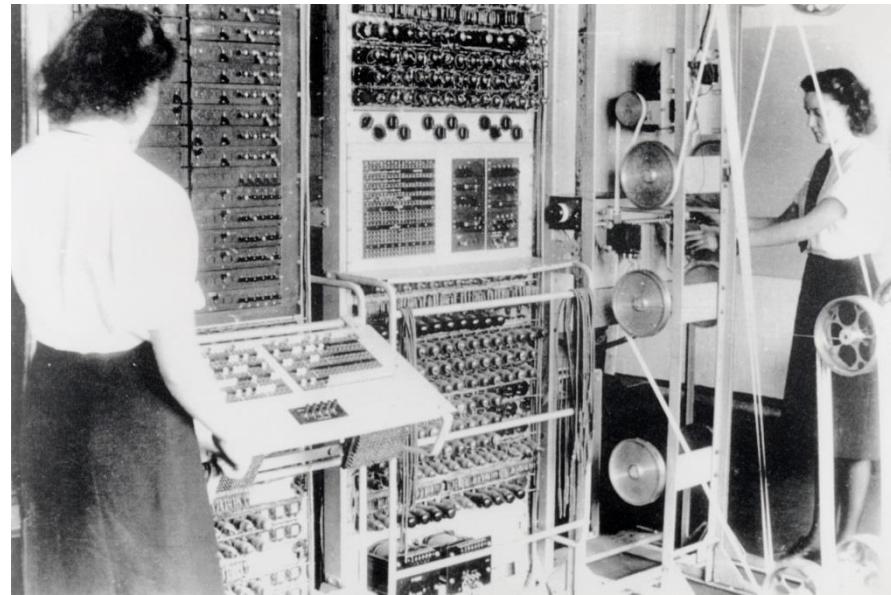
**Se parte do texto inicial ( $\text{Texto}_0$ ) for conhecido, as variações podem ser encontradas**

# Criptanálise da Tunny

- A mensagem começava com um texto padrão: **SPRUCHNUMMER** — número de mensagem
  - Na primeira vez o operador escreveu: **SPRUCHNUMMER**
  - Na segunda vez escreveu: **SPRUCHNR**
  - Assim, imediatamente após o N os dois criptogramas eram diferentes!
- As mensagens foram completamente decifradas por John Tiltman, em Bletchley Park, usando combinações aditivas dos criptogramas (chamados Depths)
  - A segunda mensagem era cerca de 500 caracteres mais curta que a primeira
- Assim se conseguiu obter, pela 1<sup>a</sup> vez, um exemplar longo de uma chave contínua Lorenz
  - Tiltman ainda não sabia como a Lorenz operava, apenas sabia que o que tinha era o resultado da sua operação!

# Tunny

- A estrutura da cifra foi deduzida da chave contínua capturada
  - Mas a decifra dependia do conhecimento da posição inicial dos rotores
- Os alemães começaram a usar números para definir o estado inicial dos rotores
  - Bill Tutte desenvolveu um método para o encontrar
  - A máquina Colossus foi desenvolvida para o aplicar
- Colossus
  - Conceção começou em março de 1943
  - O Colossus Mark 1 (1500 válvulas) operacional em jan. de 1944
  - Reduziu o tempo de criptanálise de semanas para horas



# Cifras Modernas: Tipos

- **Quanto à operação**

- Por blocos (mono-alfabéticas)
- Contínuas (poli-alfabéticas)

- **Quanto ao tipo de chave**

- Simétricas (chave secreta ou segredo partilhado)
  - Potencialmente sujeitas a caução (escrowing)
- Assimétricas (chave pública)

- **Combinatória**

	Cifras Por Blocos	Cifras Contínuas
Cifras Simétricas		
Cifras Assimétricas		NÃO EXISTEM

# Cifras Simétricas

**Chave secreta única, partilhada por 2 ou mais interlocutores**

- **Permitem**
  - Confidencialidade para todos os conhecedores da chave
  - Autenticação de mensagens (cifra por blocos)
    - Quando se usam cifras por blocos
- **Vantagens**
  - Desempenho (normalmente muito eficientes)
- **Desvantagens**
  - $N$  interlocutores, 2 a 2 secretamente  $\rightarrow N \times (N-1)/2$  chaves
- **Problemas**
  - Distribuição de chaves

# Cifras Simétricas Contínuas

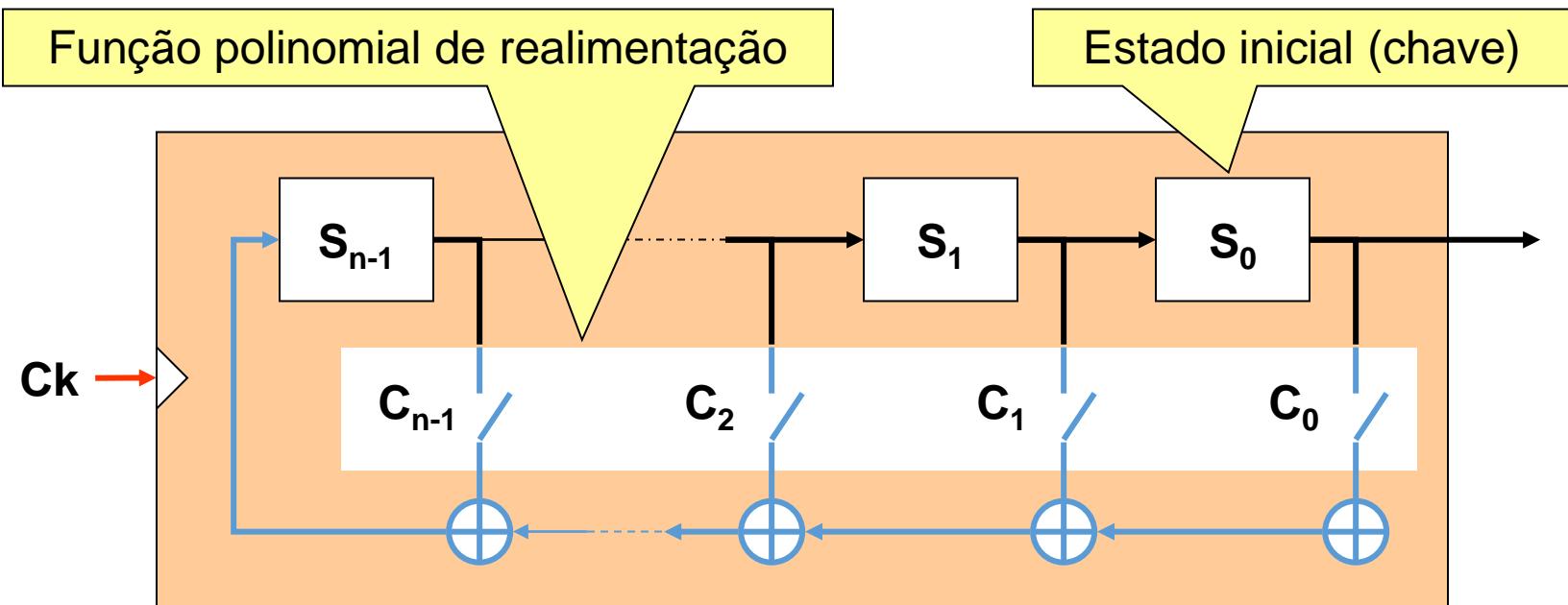
- **Aproximações usadas**

- Desenho de geradores pseudo-aleatórios seguros
  - Baseados em LFSRs
  - Baseados em cifras por blocos
  - Outras aproximações (famílias de funções, etc.)
- Normalmente são síncronas
  - Não possuem sincronização inerente, mas obrigam a que emissor/recetor estejam sincronizados.
- Normalmente sem possibilidade de acesso aleatório rápido

- **Algoritmos mais comuns**

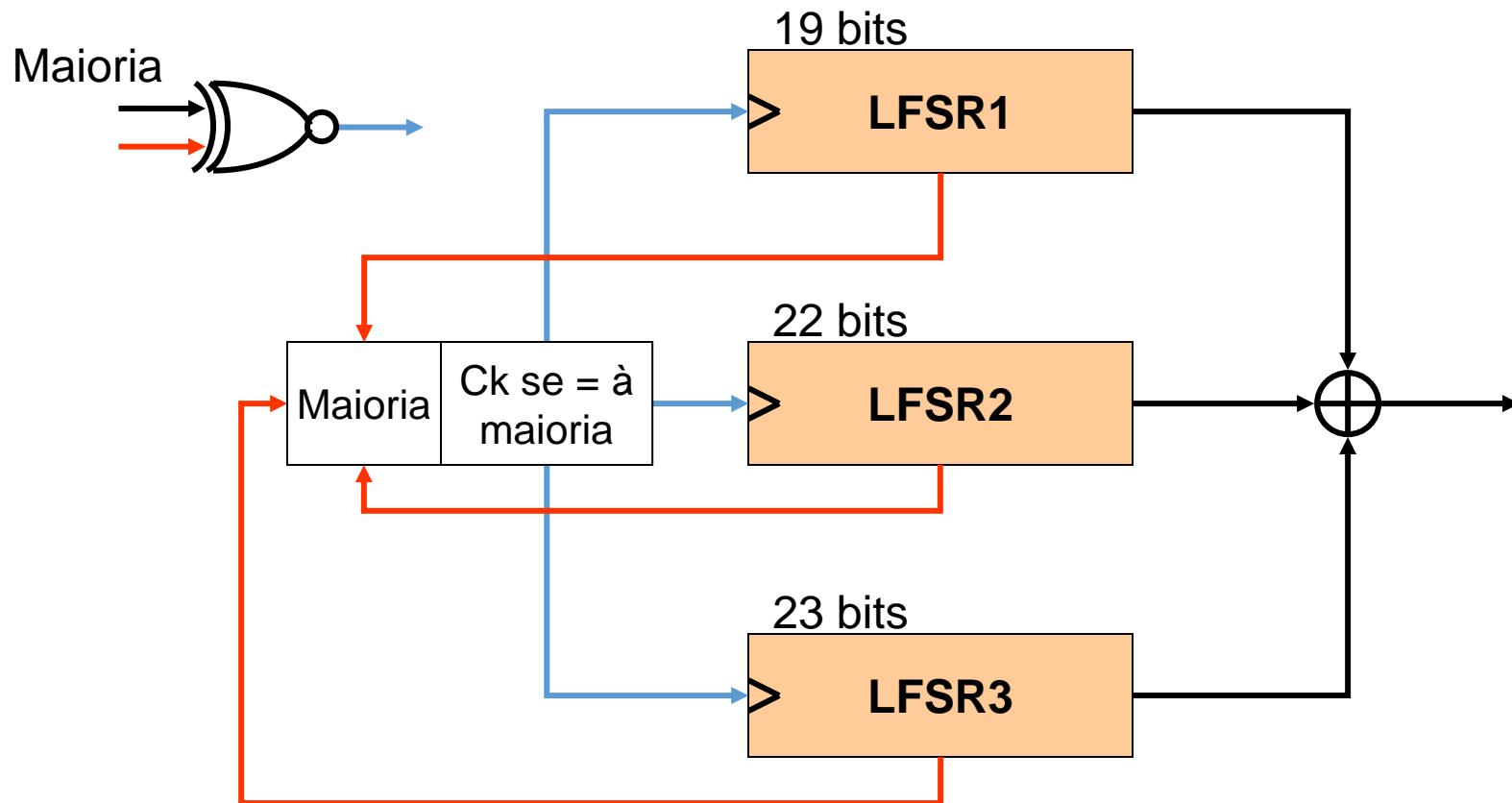
- A5/1 (US, Europe), A5/2 (GSM)
- RC4 (802.11 WEP/TKIP, etc.)
- E0 (Bluetooth BR/EDR)
- SEAL (c/ acesso aleatório uniforme)
- Chacha20
- Salsa20

# Linear Feedback Shift Register (LFSR)



- **$2^n - 1$  sequências não nulas**
  - Se uma delas possuir um período  $2^n - 1$  então todas o têm
- **Funções de realimentação primitivas (polinomiais primitivos)**
  - Todas as sequências não nulas têm comprimento  $2^n - 1$

# Geradores com composições de LFSR: A5/1 (GSM)



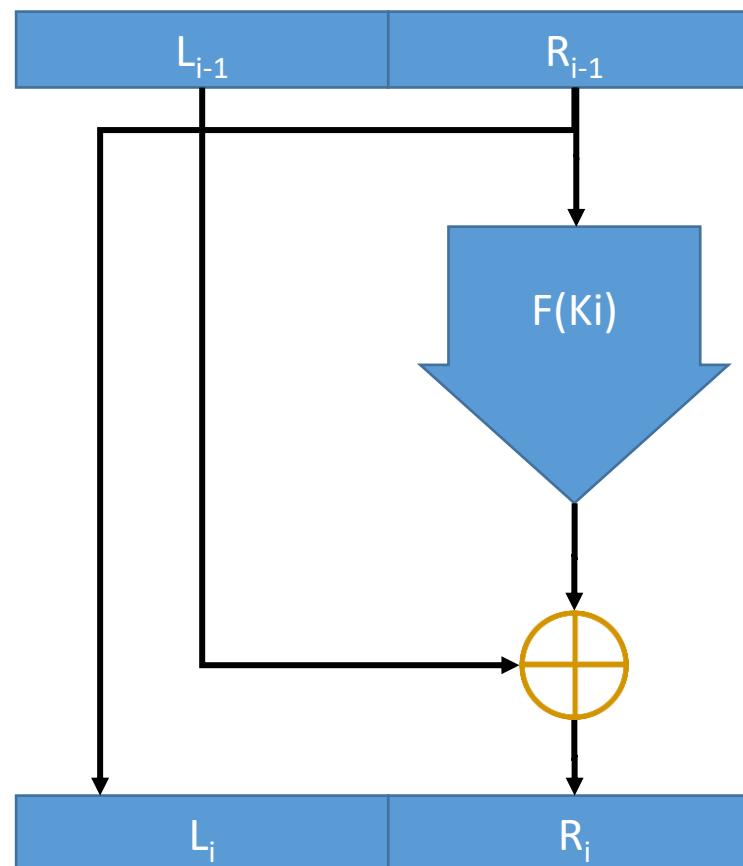
# Cifras Simétricas por Blocos

- Aproximações usadas
  - Blocos de grande dimensão, >128bits.
- Difusão, confusão
  - Permutação, substituição, expansão, compressão
  - Redes de Feistel com múltiplas iterações
    - $L_i = R_{i-1}$      $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
  - Ou redes de substituição-permutação
- Algoritmos mais usados
  - DES (Data Enc. Stand.), D=64; K=56
  - IDEA (Int. Data Enc. Alg.), D=64; K=128
  - AES (Adv. Enc. Stand., aka Rijndael), D=128, K=128, 192, 256
  - Outros (Blowfish, CAST, RC5, etc.)

# Redes de Feistel

$$L_i = R_{i-1}$$

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

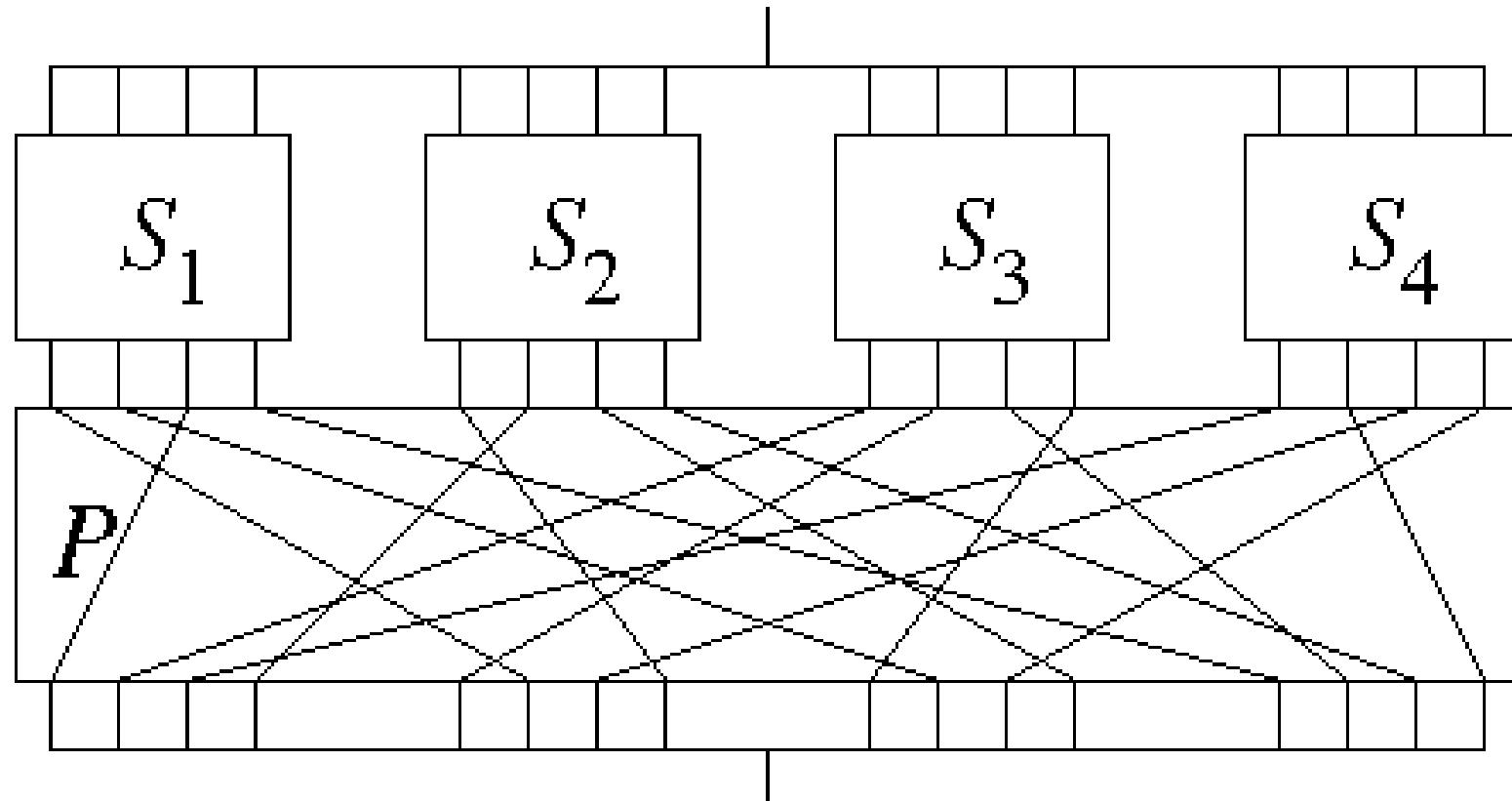


# Redes de Substituição-Permutação

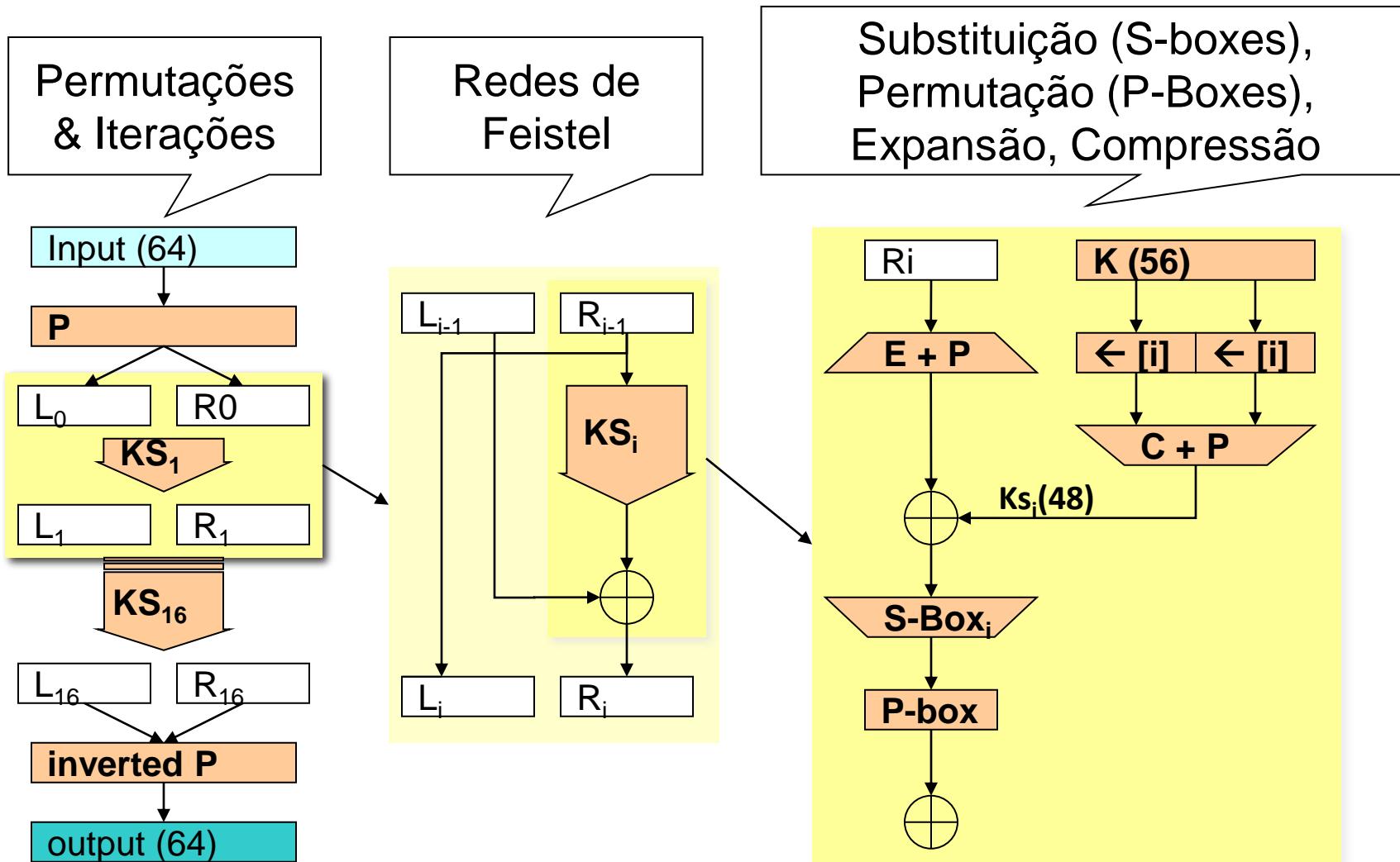
- **S-Box: (Substituição) baseado num bit da entrada, troca bits da saída**
  - substituição não é direta (1 para 1)
  - ideal: alteração de um bit provoca a alteração de todos os bits
  - prática: a alteração de um bit provoca a alteração de pelo menos metade dos bits
- **P-Box: (Permutação) - permuta a posição de bits entre entrada e saída**
  - ideal: permuta a posição de todos os bits

**Operação de ambas depende da chave**

# Redes de Substituição-Permutação



# DES: Data Encryption Standard



# DES: robustez

- **Escolha de chaves**
  - A maioria dos valores de 56 bits são adequados
  - Mas... existem 4 chaves fracas, 12 semi-fracas e 48 quasi-fracas
    - Produzem  $K_s$  semelhantes (1  $K_s$ , 2  $K_s$  ou 4  $K_s$ )
  - Fáceis de identificar e de evitar
- **Ataques conhecidos**
  - Pesquisa exaustiva (possível na prática com chaves de 56 bits)
- **Dimensão das chaves: 56 bits são atualmente insuficientes**
  - A pesquisa exaustiva é técnica e economicamente viável
- **Solução: cifra múltipla**
  - Cifra dupla não é completamente segura (teoricamente ...)
  - Cifra tripla: 3DES (Triple-DES)
    - Com duas ou três chaves
    - Chaves equivalentes de 112 ou 168 bits
    - Usando a mesma chave, o algoritmo é compatível com o DES

# Utilização de cifras por blocos: Modos

- **Processam texto em blocos de bits**
  - Texto **tem de ser múltiplo** do tamanho do bloco
  - Na prática:  $\text{size}(\text{cryptogram}) \geq \text{size}(\text{plaintext})$
- **Podem aplicar mecanismos de difusão e confusão**
  - Dentro de cada bloco
  - Mas podem ser usadas como cifras contínuas
- **Método de cifra mais comum**
  - Especialmente para objetos discretos (ficheiros, documentos)
- **Cifra mais popular: AES**

# Utilização de cifras por blocos: Modos

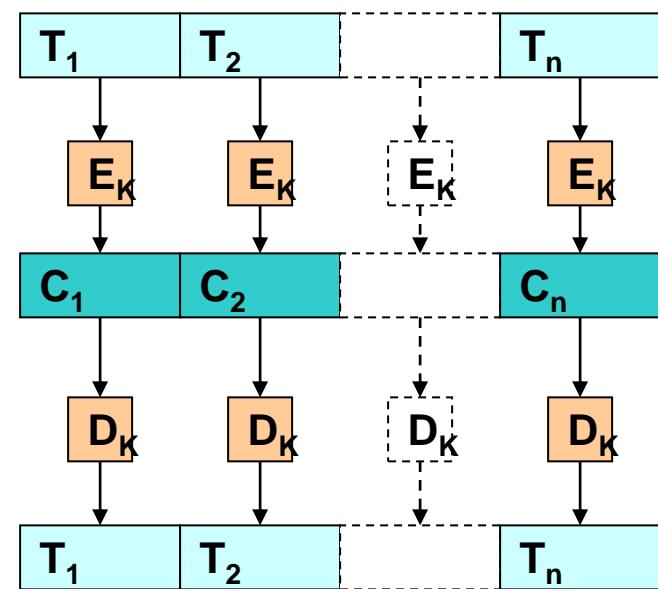
- **Propostos inicialmente para o DES**
  - ECB (Electronic Code Block)
  - CBC (Cipher Block Chaining)
  - OFB (Output Feedback Mode)
  - CFB (Cipher Feedback Mode)
- **Modos podem ser usados com outras cifras (em teoria)**
- **Podem existir outros modos:**
  - CTR (Counter Mode)
  - GCM (Galois/Counter Mode)
  - Tweaks...

# Modos: Electronic Code Block

- Cifra direta de cada bloco:  $C_i = E_k(T_i)$
- Decifra direta de cada bloco:  $T_i = D_k(C_i)$
- Blocos são independentes
  - Sem feedback

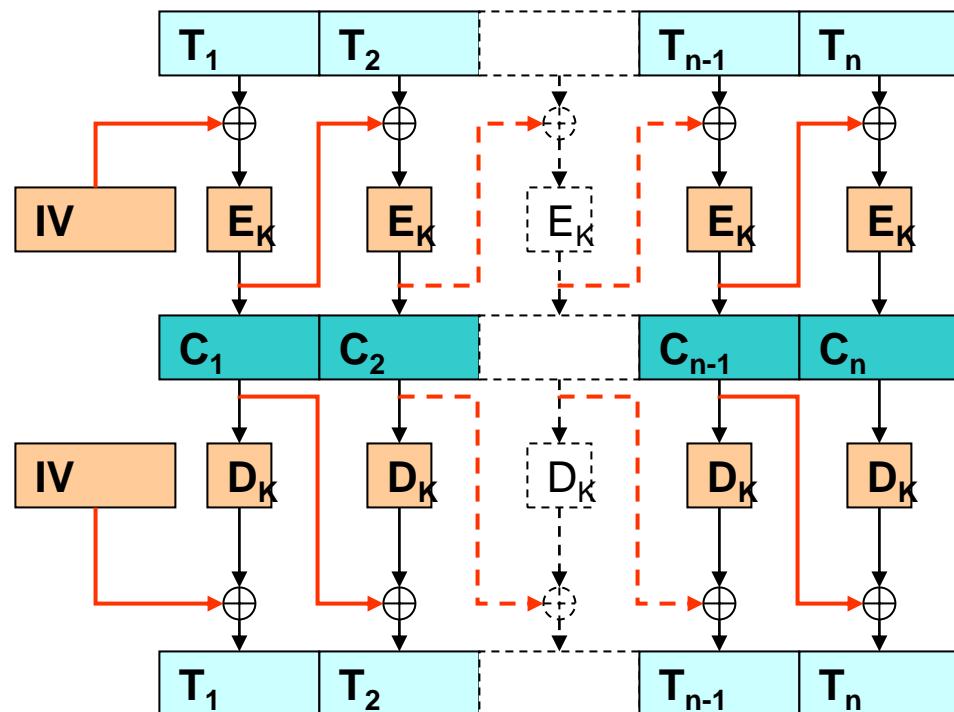
- Problema:

**se  $T_1 = T_2$  então  $C_1 = C_2$**

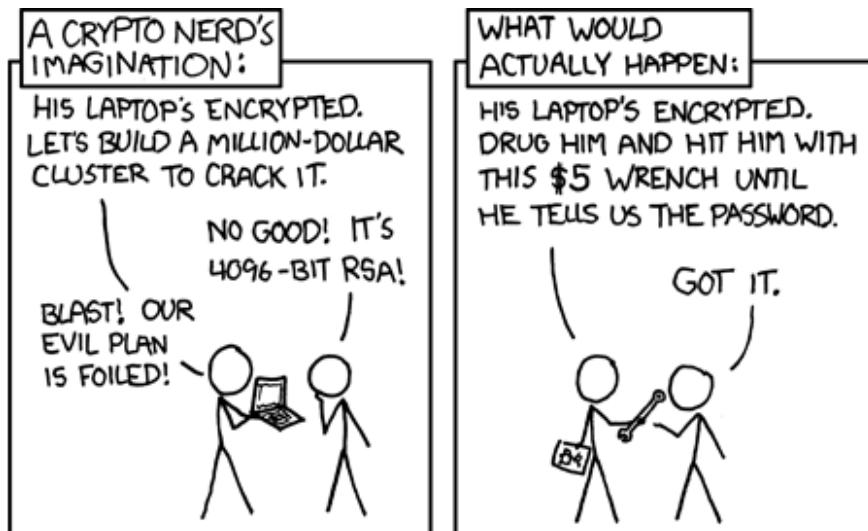


# Modos: Cipher Block Chaining (CBC)

- Cifra de cada bloco  $T_i$  com feedback de  $C_{i-1}$ 
  - $C_i = E_K(T_i \oplus C_{i-1})$
- Decifra de cada bloco  $C_i$  com feedback de  $C_{i-1}$ 
  - $T_i = D_K(C_i) \oplus C_{i-1}$
- Bloco inicial usa IV
  - Initialization Vector
  - Valor aleatório único
  - Pode estar em claro

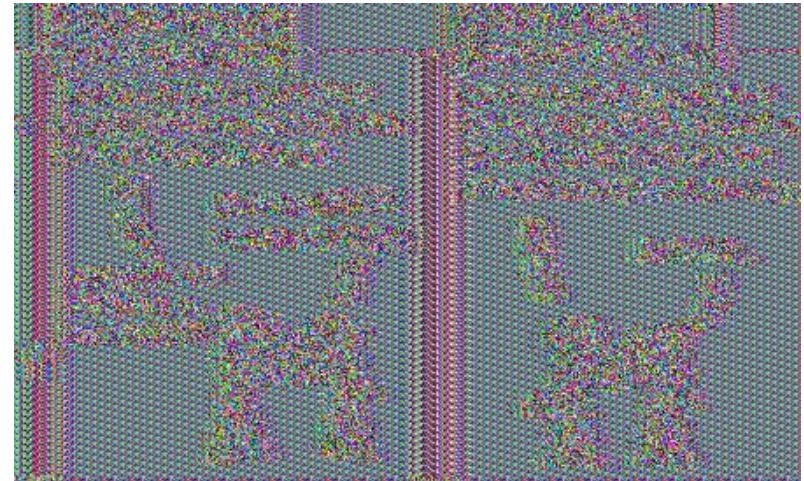


# ECB vs CBC: Propagação de Padrões

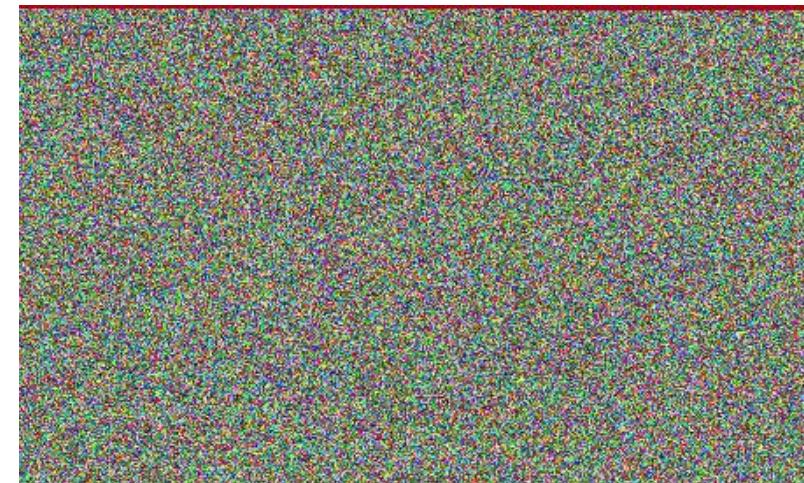


<https://xkcd.com/538/>

**ECB**



**CBC**

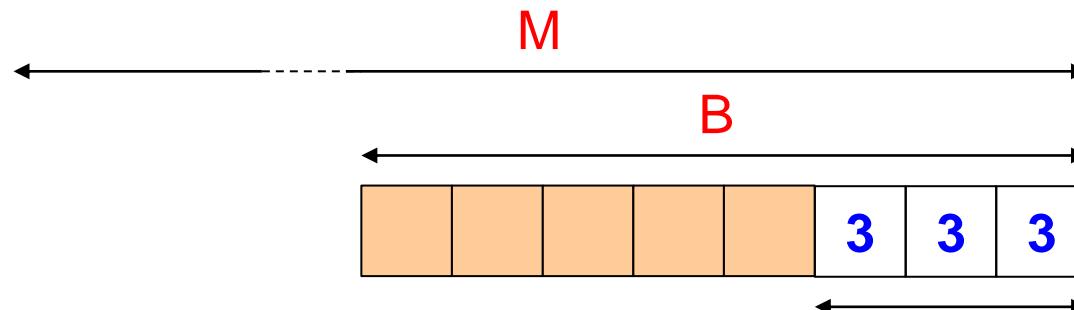


# Modos: ECB/CBC problemas de alinhamento

- **Modos ECB/CBC necessitam de textos com dimensão múltipla da dimensão do bloco**
  - Cifra é aplicada por blocos de texto
- **Blocos incompletos (o último) necessitam de tratamento diferenciado**
  - na cifra e na decifra
- **Resultado é um bloco**
  - Criptograma pode ser maior do que o texto em claro

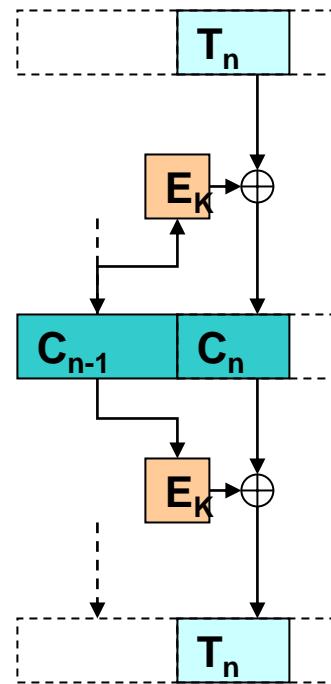
# Modos: ECB/CBC problemas de alinhamento

- Alternativa: Excipiente (Padding)
- PKCS #7
  - $X = B - (M \bmod B)$
  - X bytes extra, com valor X
  - Se  $M \bmod B = 0$ , adicionar um bloco inteiro com valor B
- PKCS #5: igual a PKCS#7 mas só para B=8



# Modos: ECB/CBC problemas de alinhamento

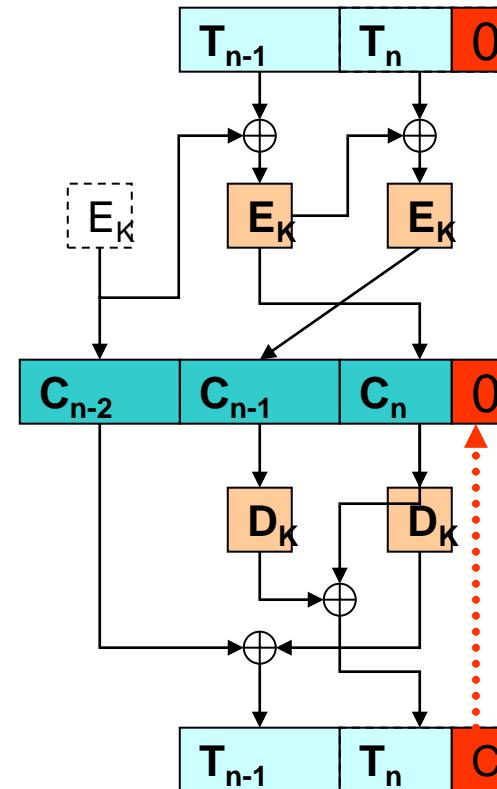
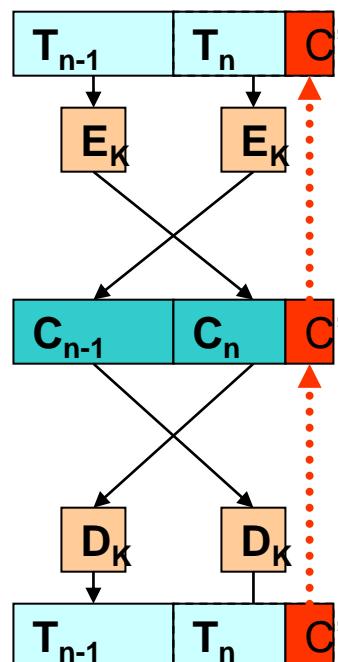
- Cifrar o último bloco de forma diferenciada
  - usar um processo semelhante a uma cifra contínua



# Modos: ECB/CBC problemas de alinhamento

- **Ciphertext Stealing**

- Troca ordem de cifra/decifra dos dois últimos blocos
  - a) Usa parte do criptograma do penúltimo para preencher último
  - b) Usa excipiente fixo e cifra contínua antes de cifra por blocos



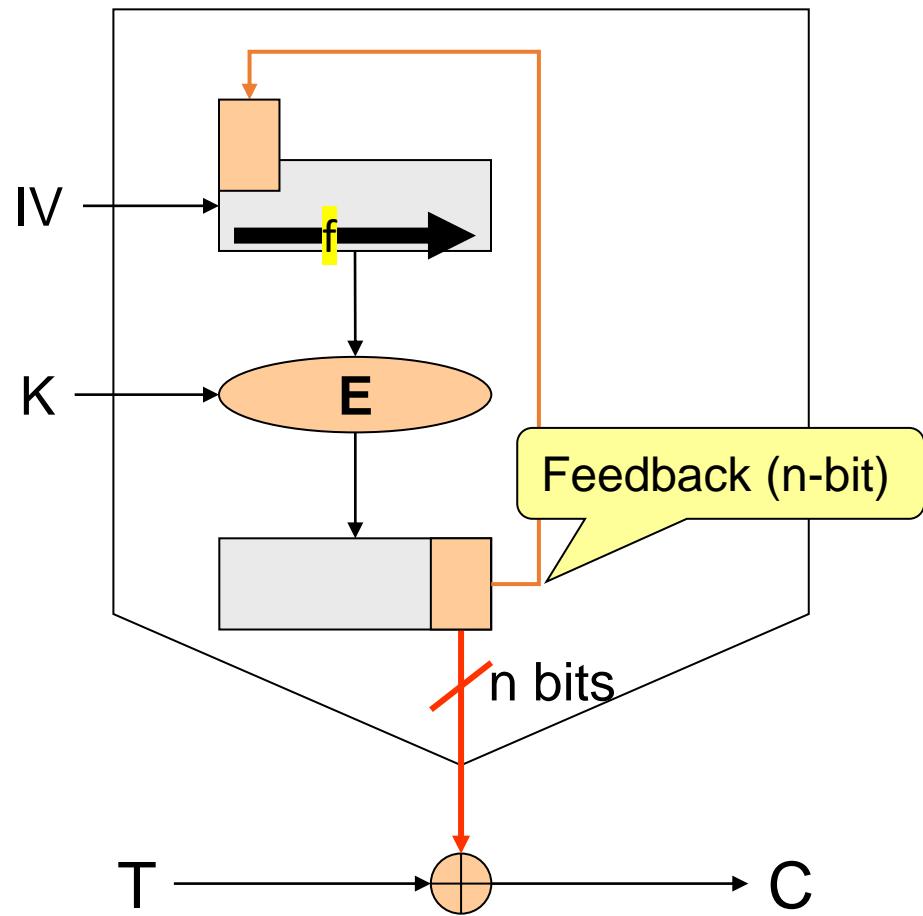
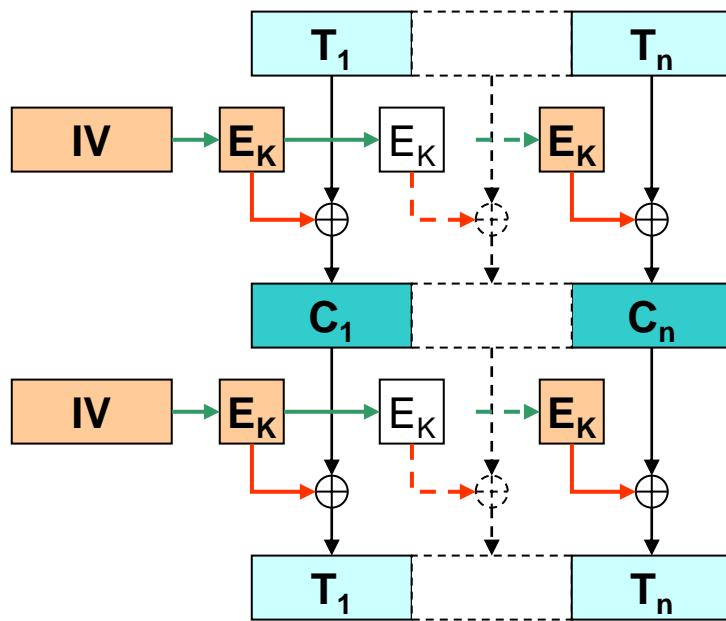
# Modos: n-bit OFB (Output Feedback)

$$C_i = T_i \oplus E_K(S_i)$$

$$T_i = C_i \oplus E_K(S_i)$$

$$S_i = f(S_{i-1}, E_K(S_{i-1}))$$

$$S_0 = IV$$

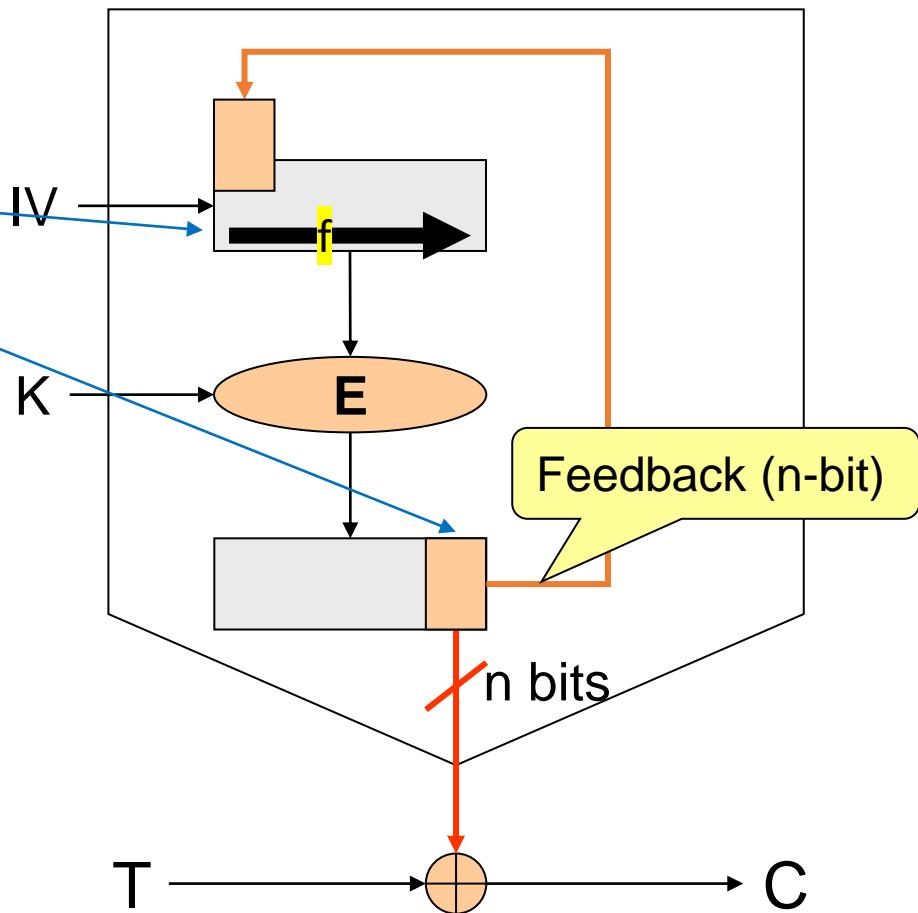
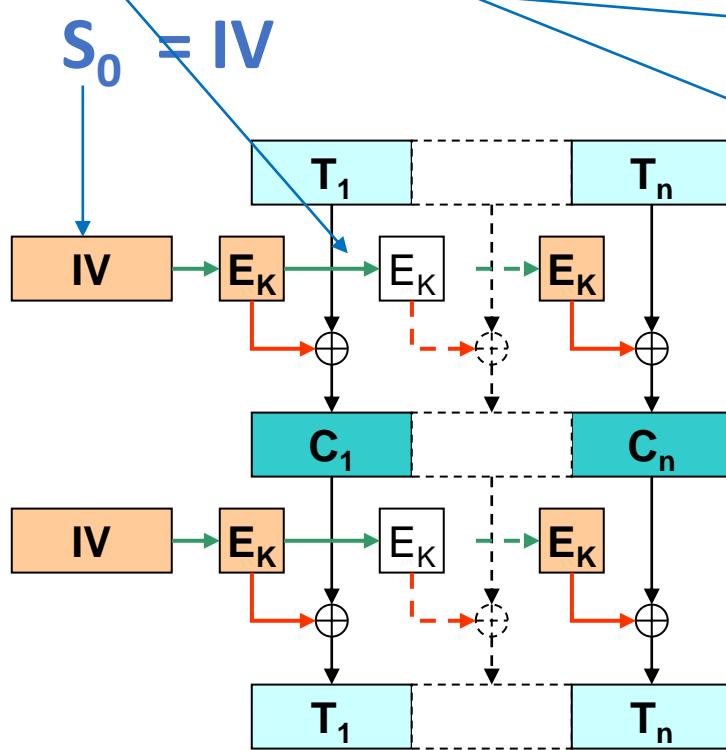


# Modos: n-bit OFB (Output Feedback)

$$C_i = T_i \oplus E_K(S_i)$$

$$T_i = C_i \oplus E_K(S_i)$$

$$S_i = f(S_{i-1}, E_K(S_{i-1}))$$



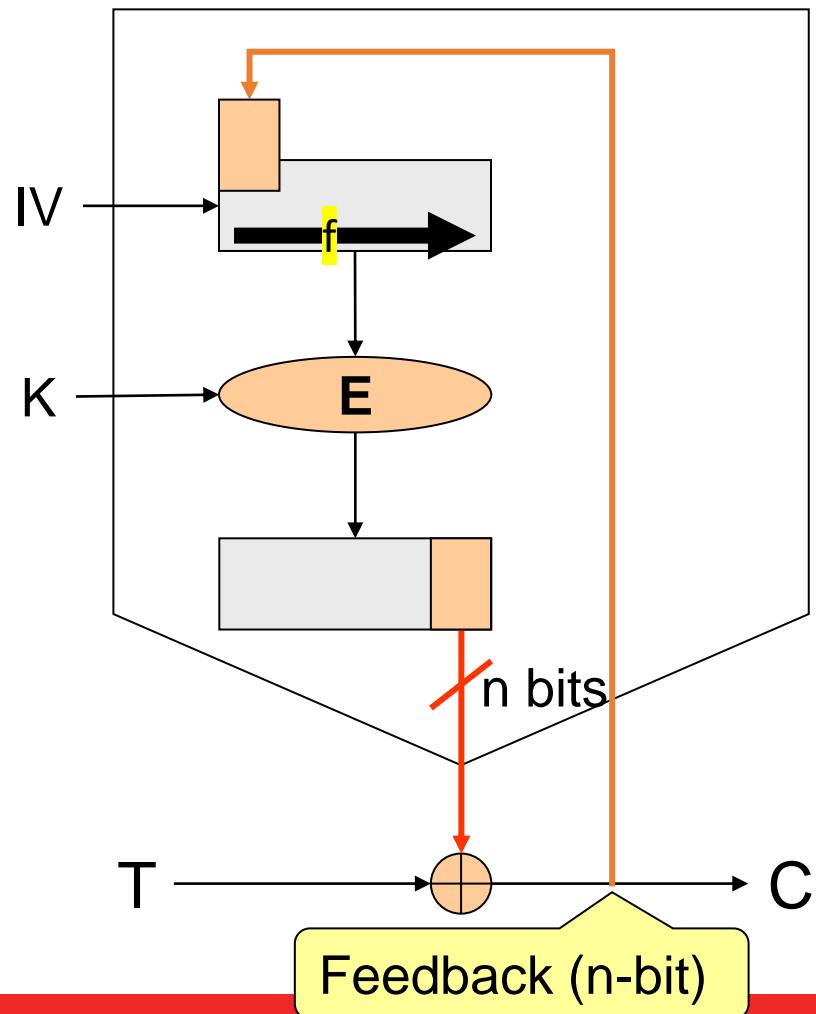
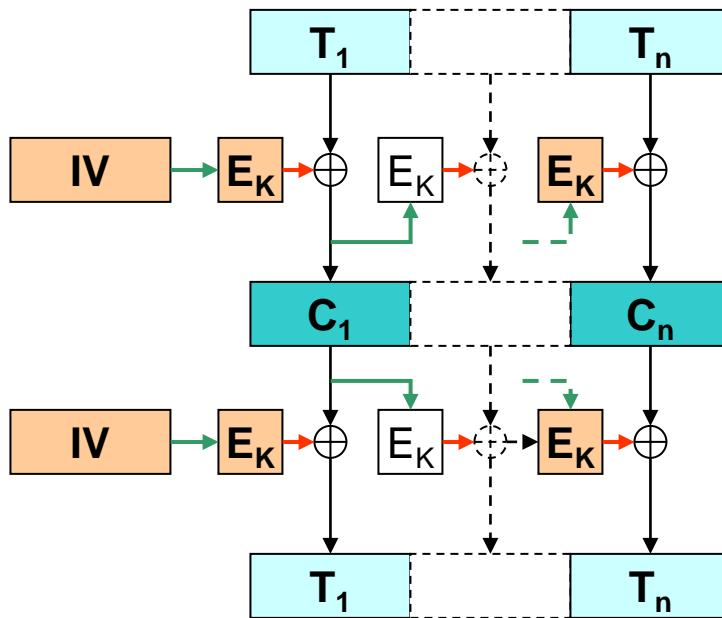
# Modos: n-bit CFB (Ciphertext Feedback)

$$C_i = T_i \oplus E_K(S_i)$$

$$T_i = C_i \oplus E_K(S_i)$$

$$S_i = f(S_{i-1}, C_i)$$

$$S_0 = IV$$



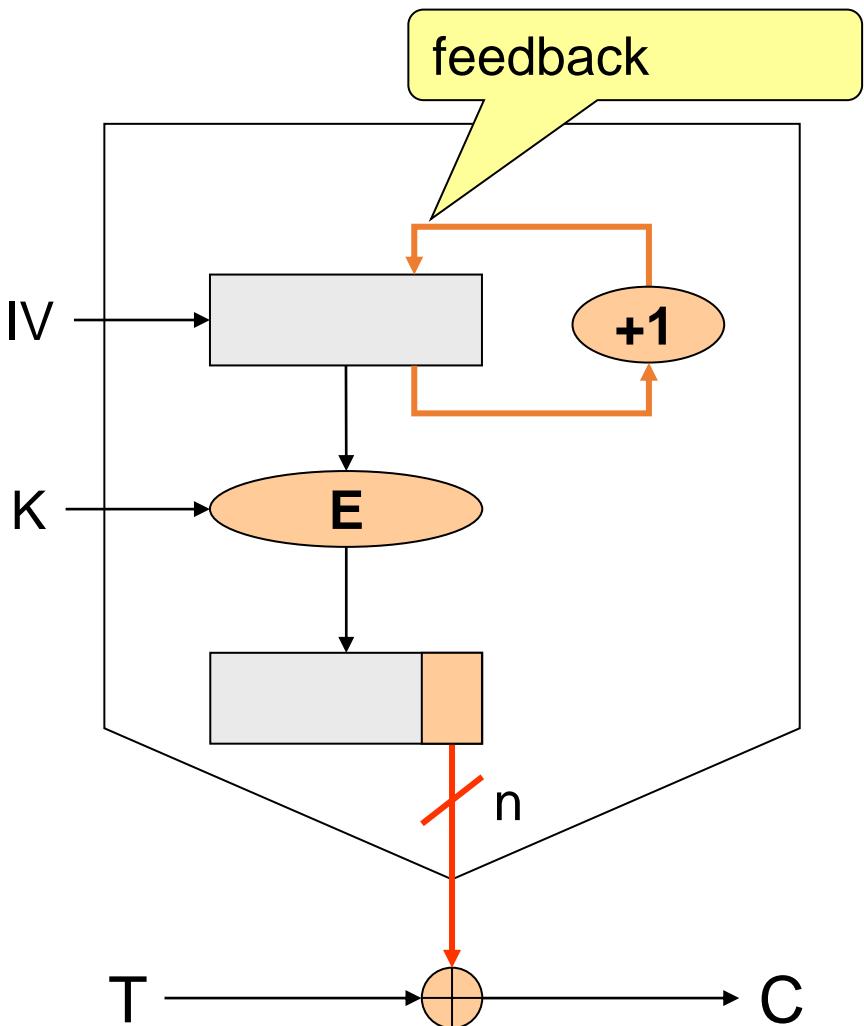
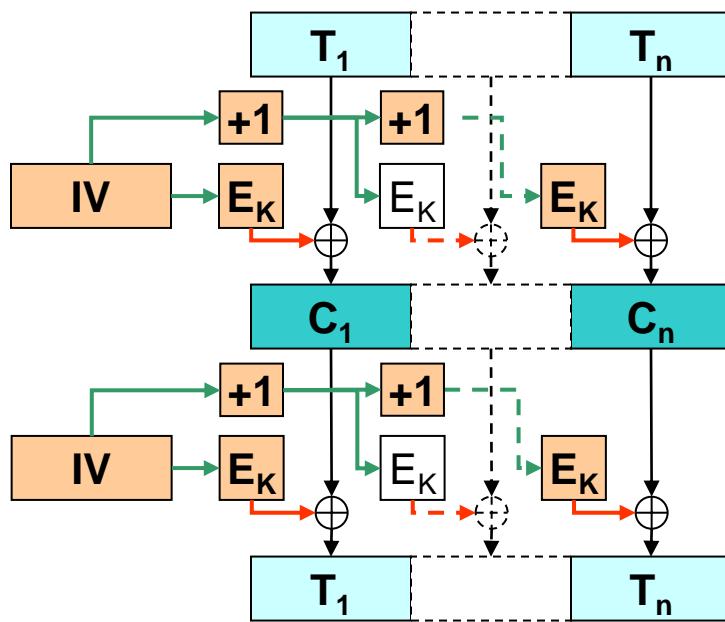
# Modos: n-bit CTR (Counter)

$$C_i = T_i \oplus E_K(S_i)$$

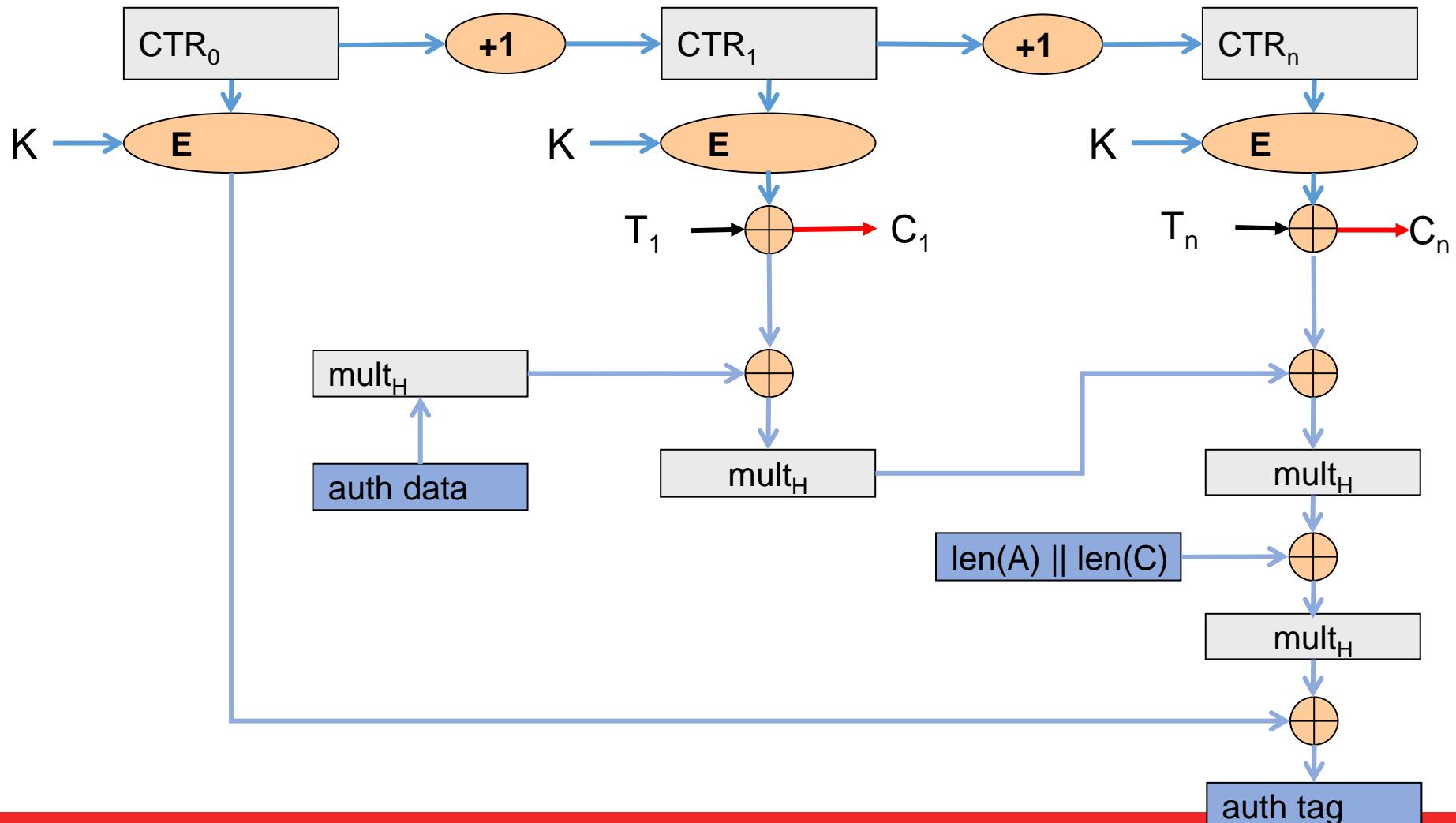
$$T_i = C_i \oplus E_K(S_i)$$

$$S_i = S_{i-1} + 1$$

$$S_0 = IV$$



# Modos: Galois w/ Counter Mode (GCM)



# Modos: Comparação

	Bloco		Contínua (Stream)			
	ECB	CBC	OFB	CFB	CTR	GCM
Ocultação de padrões no texto		✓	✓	✓	✓	✓
Confusão na entrada da cifra		✓		✓	Contador Secreto	Contador Secreto
Mesma chave para mensagens diferentes	✓	✓	Outro IV	Outro IV	Outro IV	Outro IV
Dificuldade de alteração	✓	✓ (...)				✓
Pré-processamento			✓		✓	✓
Paralelização	✓	decifra	com pré. proc.	decifra	✓	✓
Acesso aleatório uniforme						
Propagação de erros		próximo bloco		alguns bits seguintes		detetado
Capacidade de re-sincronização	perda de blocos	perda de blocos		perda de múltiplos n-bits		detetado

# Modos: Reforço da Segurança

## Cifra Múltipla

- **Cifra dupla**
  - Violável por intromissão em  $2^{n+1}$  tentativas
    - Com 2 ou mais blocos de texto conhecido
    - Usando  $2^n$  blocos de memória ...
  - Não é (teoricamente) muito mais segura ...
- **Cifra tripla (EDE):**  $C_i = E_{K1}(D_{K2}(E_{K3}(T_i)))$        $P_i = D_{K3}(E_{K2}(D_{K1}(C_i)))$ 
  - Normalmente usa-se  $K_1=K_3$
  - Se  $K_1=K_2=K_3$  transforma-se numa cifra simples

# Modos: Reforço da Segurança (Cifra dupla)

## Ataque Meet in The Middle

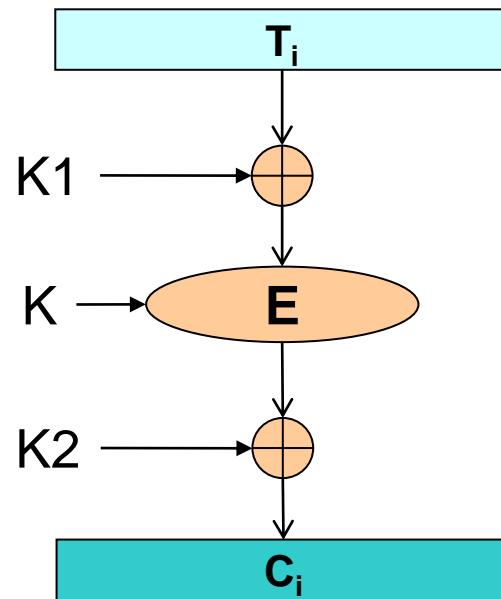
- **Cifra dupla com duas chaves  $K_a$  e  $K_b$** 
  - $C = E_b(k_b, E_a(k_a, T))$
  - $T = D_a(k_a, D_b(k_b, C))$
  - Logo:  $D_b(k_b, C) = E_a(k_a, T)$
- **Se  $C$  e  $T$  forem conhecidos, podem-se calcular:**
  - Todos os valores  $D_b(k_b, C)$ , variando  $K_b$
  - Todos os valores  $E_a(k_a, T)$ , variando  $K_a$
- **Chaves encontradas quando se verificar a igualdade**
  - Complexidade esperada:  $2^{\text{len}(k_a) + \text{len}(k_b)}$
  - Complexidade real:  $2^{\text{len}(k_a)} + 2^{\text{len}(k_b)}$
  - Exemplo para chaves de 56 bits:  $2^{56+56} = 2^{112}$  vs  $2^{56} + 2^{56} = 2^{57}$ 
    - Consumindo  $2^{56}$  bits de armazenamento (8 PiB)

# Modos: Reforço da Segurança

## Branqueamento/whitening

Técnica simples e eficiente de introdução de confusão

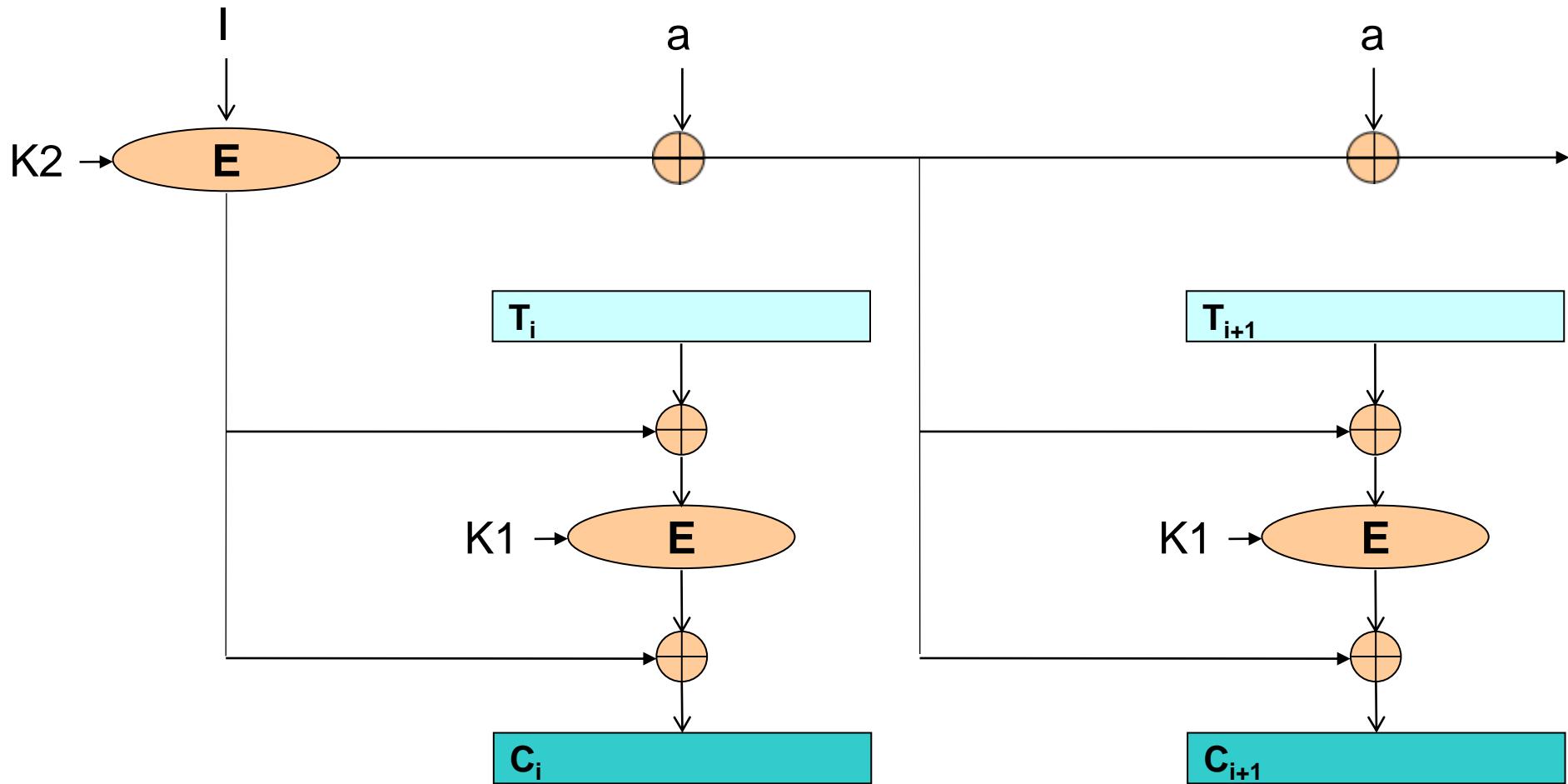
- $C_i = E_K(K_1 \oplus T_i) \oplus K_2$
- $T_i = K_1 \oplus D_K(K_2 \oplus C_i)$



# Modos: Reforço da Segurança

## XOR-Encrypt-XOR (XEX)

XTS = XEX + Ciphertext Stealing



# Cifras Assimétricas por Blocos

- **Par de chaves**
  - Uma privada, pessoal e intransmissível
  - Uma pública, disponível para todos
- **Permitem**
  - Confidencialidade sem troca de segredos
  - Autenticação de conteúdos (**integridade**) e de autoria (**assinaturas digitais**)

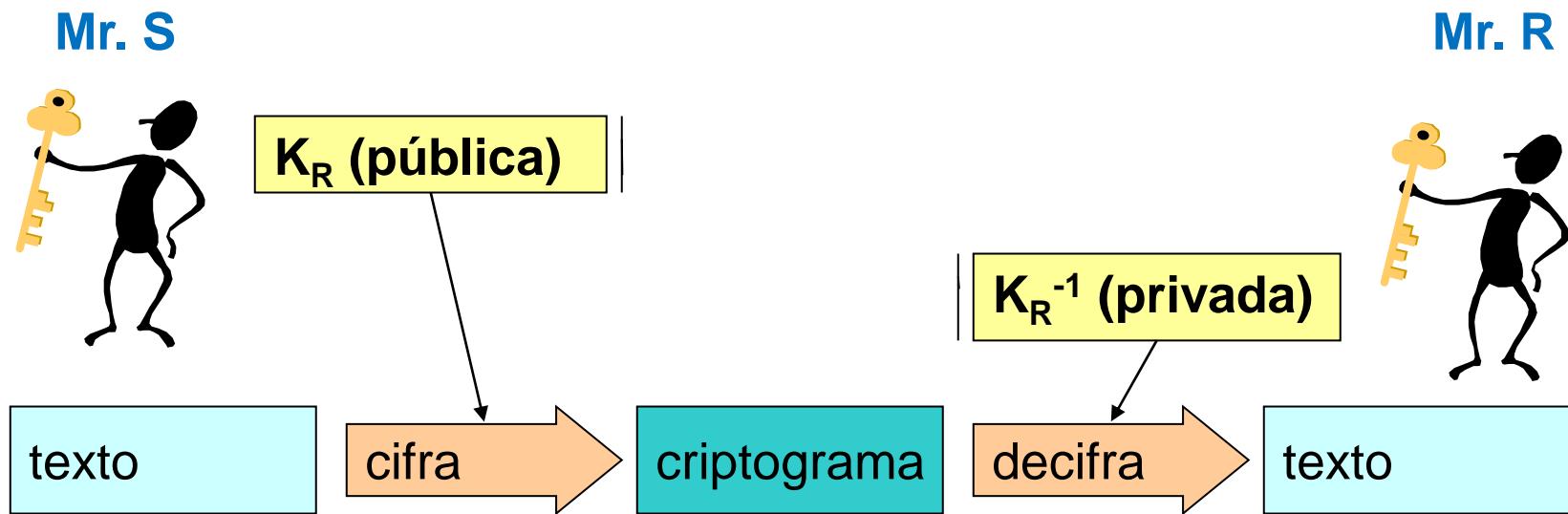
# Cifras Assimétricas por Blocos

- **Desvantagens**
  - Desempenho (normalmente pouco eficientes)
- **Vantagens**
  - Interação com N interlocutores requer apenas N pares de chaves
    - Cifra por blocos simétrica iria requerer  $N^2$
- **Problemas**
  - Distribuição de chaves públicas (têm de ser distribuídas à priori)
  - Tempo de vida dos pares de chaves (têm de expirar)

# Cifras Assimétricas por Blocos

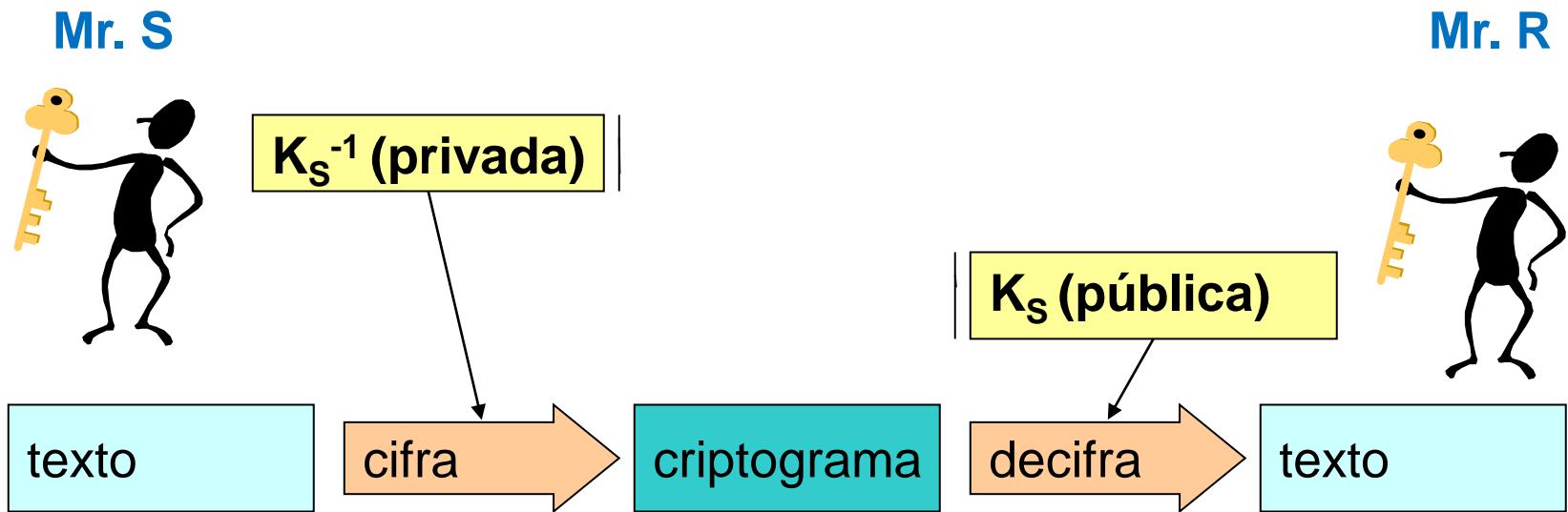
- **Aproximações: complexidade matemática**
  - Cálculo de logaritmos discretos
  - Fatorização de grandes números
  - Problema da mochila (knapsack)
- **Algoritmos mais usados**
  - RSA
  - ElGamal
  - Curvas elípticas (Elliptic Curve Cryptography, ECC)
- **Outras técnicas com chave pública**
  - Diffie-Hellman (negociação de chaves)

# Confidencialidade c/ Cif. Assimétricas



- **Menos chaves**
  - $C = E(K, P)$   $P = D(K^{-1}, C)$
  - Para ter confidencialidade basta **R** conhecer a chave pública de **R** ( $K_R$ )
- **Não há autenticação de origem**
  - **R** não sabe quem produziu o criptograma
  - Se  $K_R$  for efetivamente pública, qualquer um o pode fazer

# Autenticidade c/ Cif. Assimétricas



- O criptograma não pode ser alterado
  - $C = E(K^{-1}, P)$   $P = D(K, C);$
  - Só S conhece a chave  $K_S^{-1}$  com que o criptograma foi gerado
- Não há confidencialidade
  - Quem conhecer  $K_S$  decifra o criptograma
  - Se  $K_S$  for verdadeiramente pública, qualquer um o pode fazer

# RSA (Rivest, Shamir, Adelman) 1978

- **Complexidade matemática**

- Dificuldade de Fatorização de grandes números
- Dificuldade de cálculo de logaritmos discretos

- **Operações e chaves**

- $K = (e, n)$     $K^{-1} = (d, n)$
- $C = P^e \text{ mod } n$                            $P = C^d \text{ mod } n$
- $C = P^d \text{ mod } n$                            $P = C^e \text{ mod } n$

- **Escolha dos valores das chaves**

- $n$  de grande dimensão (centenas ou milhares de bits)
- $n = p \times q$                                    $p$  e  $q$  primos, de grande dimensão
- Escolher  $e$  coprimo de  $(p-1) \times (q-1)$
- Procurar um  $d$  tal que  $e \times d \equiv 1 \pmod{(p-1) \times (q-1)}$
- Não se consegue deduzir  $d$  a partir de  $e$  ou de  $n$

# RSA (Rivest, Shamir, Adelman) 1978

- $p = 5$   $q = 11$  (pequenos números primos)
  - $n = p \times q = 55$
  - $(p-1)(q-1) = 40$
- $e = 3$ 
  - Coprimo de 40
- $d = 27$ 
  - $e \times d \equiv 1 \pmod{40}$
- $P = 26$  (note que  $P, C \in [0, n-1]$ )
  - $C = P^e \pmod{n} = 26^3 \pmod{55} = 31$
  - $P = C^d \pmod{n} = 31^{27} \pmod{55} = 26$

# Diffie-Hellman

alice



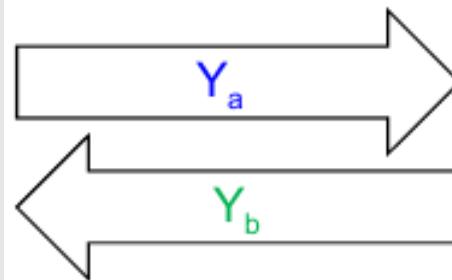
bob



$q$  (primo de elevada dimensão)  
 $\alpha$  (raiz primitiva mod  $q$ )

**a = random**

$$Y_a = \alpha^a \text{ mod } q$$



$$K_{ba} = Y_b^a \text{ mod } q$$

**b = random**

$$Y_b = \alpha^b \text{ mod } q$$

$$K_{ab} = Y_a^b \text{ mod } q$$

$$K_{ba} = K_{ab}$$

ções

# Diffie-Hellman - Ataque por MitM

alice



**a** = random

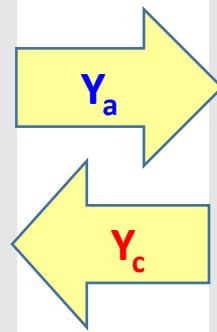
$$Y_a = \alpha^a \text{ mod } q$$

mallory



**c** = random

$$Y_c = \alpha^c \text{ mod } q$$



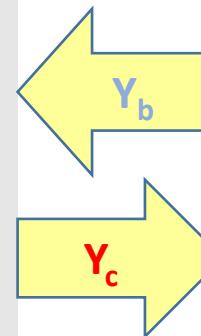
$$K_{ca} = Y_c^a \text{ mod } q$$

bob



**b** = random

$$Y_b = \alpha^b \text{ mod } q$$



$$K_{ac} = Y_a^c \text{ mod } q$$

$$K_{cb} = Y_b^c \text{ mod } q$$

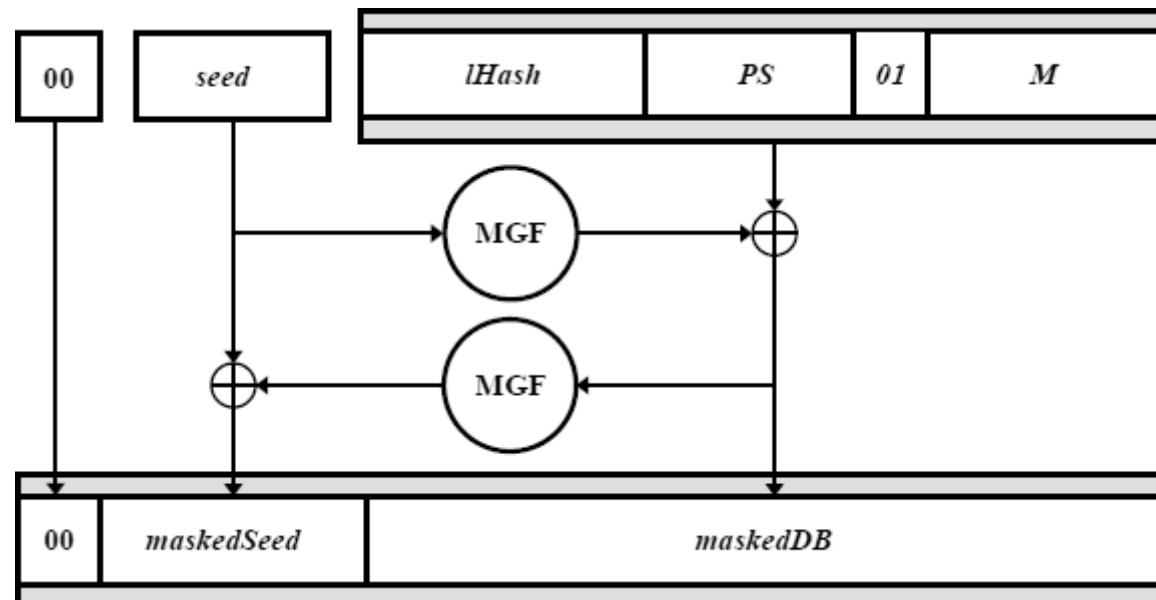
$$K_{cb} = Y_c^b \text{ mod } q$$

# Randomização de cifras com chave pública

- O resultado de uma cifra com chave pública não deverá ser determinístico (previsível)
  - N cifras do mesmo valor, com a mesma chave, devem produzir N resultados diferentes
  - Objetivo: impedir a descoberta de valores cifrados por tentativa e erro
- Técnicas
  - Concatenação do valor a cifrar com dois valores
    - Um fixo (para controlo de erros)
    - Um aleatório (para randomização)

# Randomização de cifras com chave pública: OEAP Optimal Asymmetric Encryption Padding

- IHash: Digest sobre Label
- seed: Valor aleatório
- PS: zeros
- M: Texto
- MGF: Mask Generation Function



# Aumento de performance: Cifra Híbrida

- **Combinação de Cifra Assimétrica com Simétrica**
  - Usar o melhor de dois mundos, evitando os problemas
  - Cifra Assimétrica: utilização de chaves públicas (**mas lenta**)
  - Cifra Simétrica: Rápida (**mas com fraca troca de chaves**)
- **Aproximação:**
  1. Obter  $K_{\text{pub}}$  do destinatário
  2. Gerar  $K_s$  de forma **aleatória**
  3. Calcular  $C_1 = E_{\text{sym}}(K_s, T)$
  4. Calcular  $C_2 = E_{\text{asym}}(K_{\text{pub}}, K_s)$
  5. Enviar  $C_1 + C_2$ 
    - $C_1$  = Texto cifrado com chave simétrica
    - $C_2$  = Chave simétrica cifrada com chave pública do destinatário
      - Também pode conter o IV

# Funções de Síntese (digest)

- **Resultado de dimensão constante com entradas de dimensão variável**
  - Uma espécie de “impressão digital” dos textos
- **Resultados muito diferentes para entradas similares**
  - Funções de dispersão criptográficas unidirecionais
- **Propriedades relevantes:**
  - Resistência à descoberta de um texto
    - Dada uma síntese, é difícil encontrar um texto que o produza
  - Resistência à descoberta de um 2º texto
    - Dado um texto, é difícil encontrar um segundo texto com a mesma síntese
  - Resistência à colisão
    - É difícil encontrar dois textos com a mesma síntese
    - Paradoxo do aniversário

# Funções de Síntese: Dimensão dos Textos

- Considerando o textos semelhantes, mas diferentes:
  - T1: "Hello User\_A!", T2: "Hello User\_B!", T3: "Hello User\_XY!"
- Diferentes algoritmos produzem valores de dimensão diferente, mas independente da dimensão do texto
  - MD5:
    - T1: 70df836fdaf02e0dfc990f9139762541
    - T3: a08313b553d8bf53ca7457601a361bea
  - SHA-1:
    - T1: f591aa1eabcc97fb39c5f422b370ddf8cb880fde
    - T3: c28b0520311e471200b397eaa55f1689c8866f25
  - SHA-256:
    - T1: 9649d8c0d25515a239ec8ec94b293c8868e931ad318df4ccd0dff67aff89905
    - T3: 8fc49cde23d15f8b9b1195962e9ba517116f45661916a0f199fcf21cb686d852

# Funções de Síntese: Diferença entre Textos

- Considerando o textos semelhantes, mas diferentes:
  - T1: "Hello User\_A!", T2: "Hello User\_B!", T3: "Hello User\_XY!"
- Uma pequena alteração no texto (1 bit) produz uma alteração drástica no resultado
  - MD5:
    - T1: 70df836fdaf02e0dfc990f9139762541
    - T2: c32e0f62a7c9c815063d373acac80c37
  - SHA-1:
    - T1: f591aa1eabcc97fb39c5f422b370ddf8cb880fde
    - T2: bab31eb62f961266758524071a7ad8221bc8700b
  - SHA-256:
    - T1: 9649d8c0d25515a239ec8ec94b293c8868e931ad318df4ccd0dff67aff89905
    - T2: e663a01d3bec4f35a470aba4baccece79bf484b5d0bffa88b59a9bb08707758a

# Funções de Síntese (digest)

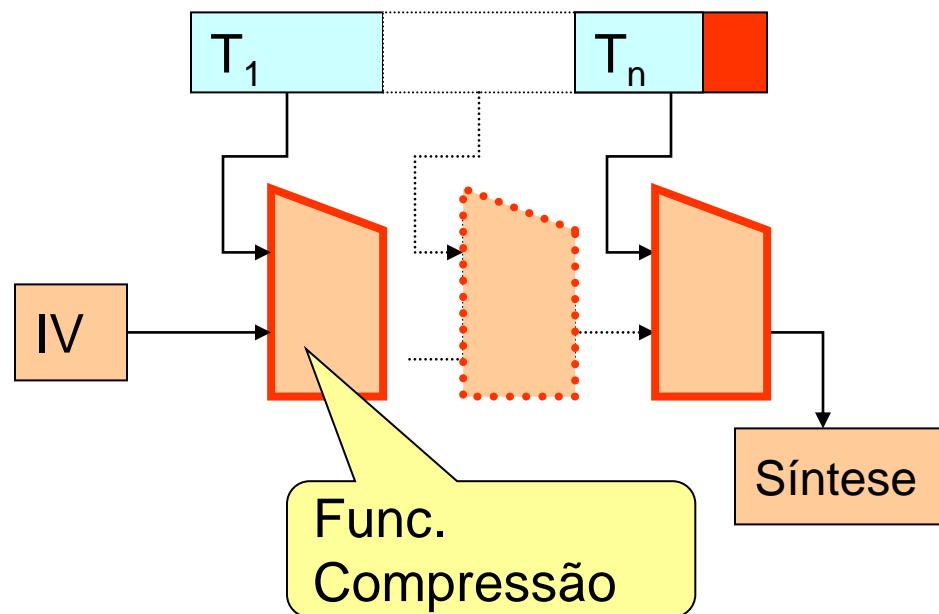
- **Aproximações**

- Difusão e confusão em funções de compressão
- Construção Merkle-Damgård
  - Compressão iterativa
  - Padding com o comprimento

- **Algoritmos mais comuns**

- MD5 (128 bits)
  - Já não é seguro! É fácil descobrir colisões!
- SHA-1 (Secure Hash Algorithm, 160 bits)
  - Já não é seguro! É fácil descobrir colisões! (em 2017)
- **SHA-2, aka SHA-256/SHA-512, SHA-3, etc.**

# Funções de Síntese

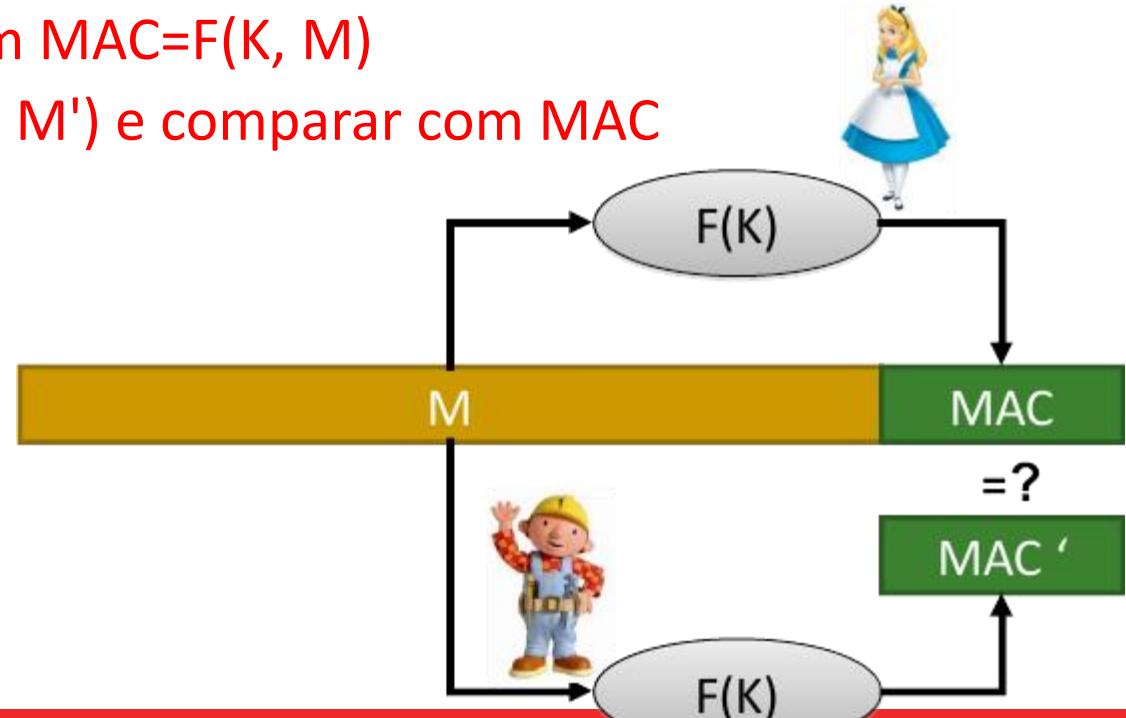


# Message Integrity Code (MIC)

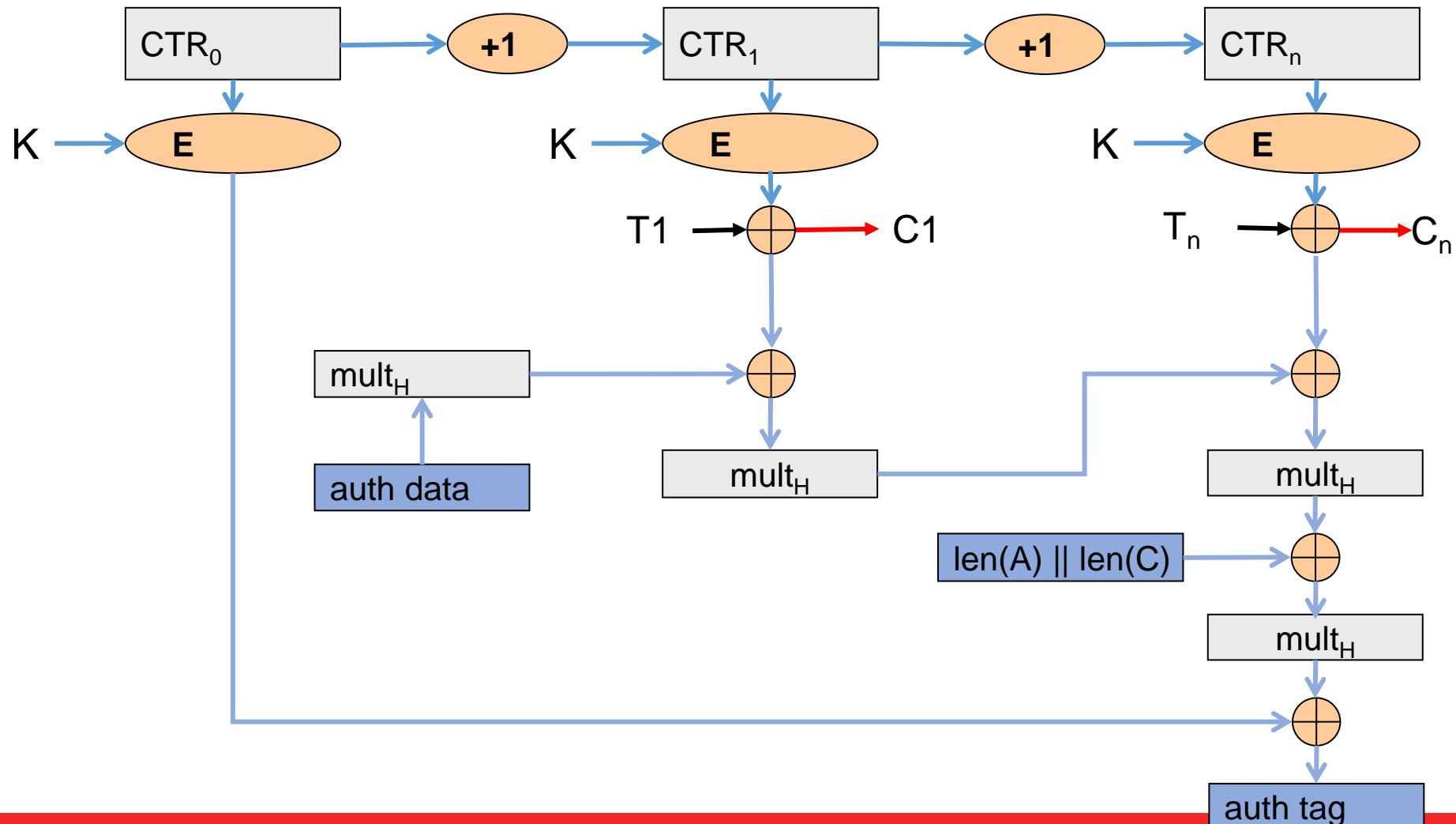
- **Forneçem capacidade de detetar alterações por máquinas**
  - Erros de comunicação/armazenamento
  - De caráter aleatório ou não controlado
- **Envio: Calcular MIC e enviar T + MIC**
  - com T=texto e MIC=síntese(T)
- **Receção: Receber dados (T') e verificar se S(T') = MIC**
  - Calcular S'=síntese(T')
  - Validar se S(T') == MIC
- **Não protege contra alterações deliberadas**
  - Atacante pode manipular T em T' e calcular novo MIC

# Message Authentication Code (MAC)

- Síntese/digest/hash gerada com recurso a uma chave
  - Só os conhecedores da chave conseguem gerar/validar o MAC
- Utilizada para garantir autenticidade/integridade
  - Enviar:  $M + MAC$ , com  $MAC = F(K, M)$
  - Receber: Calcular  $F(K, M')$  e comparar com MAC



# MAC: Cifras com Autenticação (GCM)



# MAC: Aproximações

- **Cifrando uma síntese normal**
  - Por exemplo, com uma cifra simétrica por blocos
- **Usando uma função chaveada, realimentação e propagação de erros**
  - ANSI X9.9 (ou DES-MAC) com DES CBC (64 bits)
- **Usando uma chave nos parâmetros da função**
  - Keyed-MD5 (128 bits): MD5(K, keyfill, texto, K, MD5fill)
- **Construção HMAC:  $H(K, opad, H(K, ipad, texto))$** 
  - ipad = 0x36 B vezes, opad = 0x5C B vezes
  - HMAC-MD5, HMAC-SHA, etc.

# Cifra e Autenticação

- Encrypt-then-MAC: MAC calculado do criptograma
  - Permite verificar a integridade antes da decifra
- Encrypt-and-MAC: MAC é calculado do texto
  - MAC não é cifrado
  - Fornece informação acerca do texto original (se igual a outro)
- MAC-then-Encrypt: MAC é calculado do texto
  - MAC é cifrado
  - Obriga a decifra completa antes da validação do MAC
    - Erros só são detetados após a decifra e validação

# Assinaturas Digitais

- **Autenticam o conteúdo de documentos**
  - Garantem a sua integridade
- **Autenticam o autor**
  - Garantem a identidade do autor/criador
- **Previnem repudiação do conteúdo**
  - Autor não pode negar a sua criação
    - só ele tem acesso à chave privada
    - Nota: autor é quem cria o conteúdo, não quem o envia

# Assinaturas Digitais (aproximações)

- **Cifra Assimétrica sobre Síntese**
  - Síntese usada por questões de desempenho
  - Cifra assimétrica para garantir autenticidade

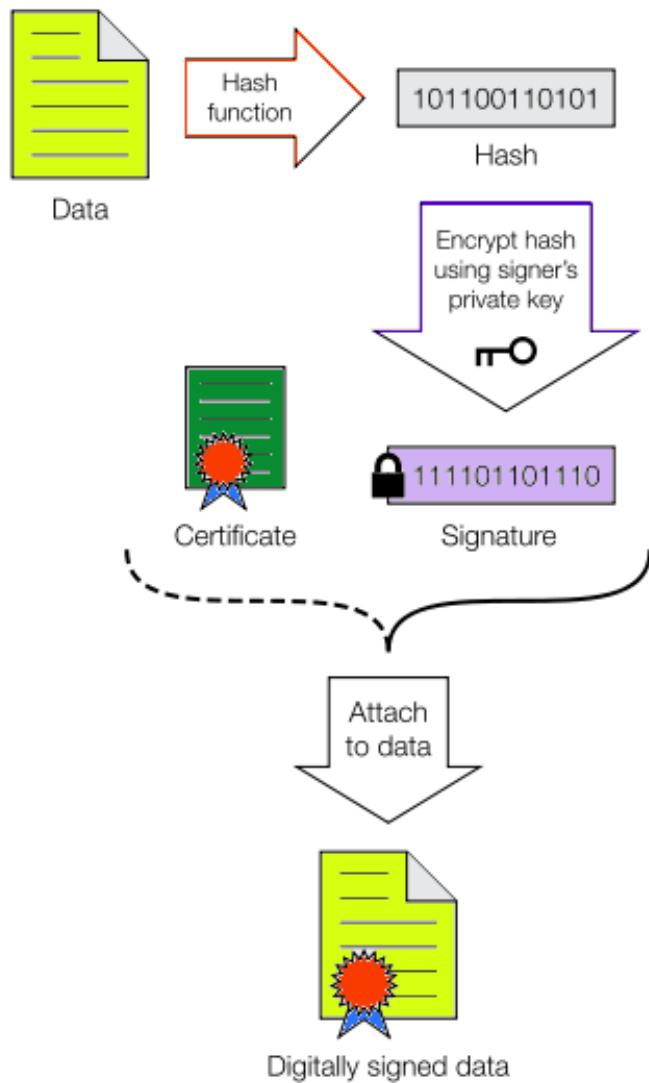
**Assinar:**  $A_x(\text{doc}) = \text{info} + E(K_x^{-1}, \text{digest(doc + info)})$

info associada com  $K_x$

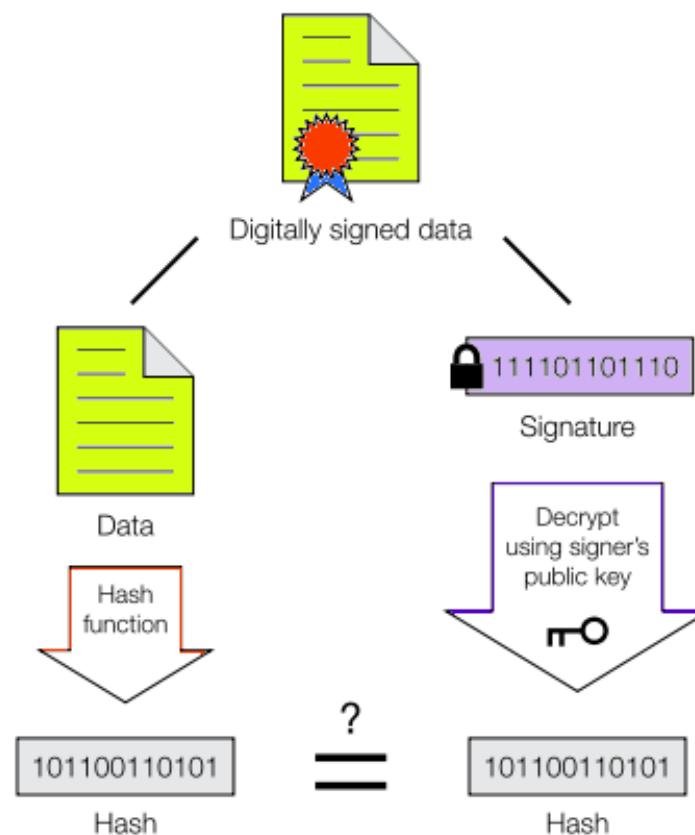
**Verificar:**

$D(K_x, A_x(\text{doc})) \equiv \text{digest(doc + info)}$

## Signing



## Verification



If the hashes are equal, the signature is valid.

# Assinatura digital num email

```
From - Fri Oct 02 15:37:14 2009
[...]
Date: Fri, 02 Oct 2009 15:35:55 +0100
From: User From <user.from@ua.pt>
Organization: UA
MIME-Version: 1.0
To: User To <user.to@ua.pt>
Subject: Teste
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=sha1; boundary="-----ms050405070101010502050101"
```

This is a cryptographically signed message in MIME format.

```
-----ms050405070101010502050101
Content-Type: multipart/mixed;
boundary="-----060802050708070409030504"
```

This is a multi-part message in MIME format.

```
-----060802050708070409030504
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable
```

Corpo do mail

```
-----060802050708070409030504-
-----ms050405070101010502050101
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature
```

```
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCggUAMIAGCSqGSIb3DQEHAQAAoIIamTCC
B1jkwgSYoAMCAQICBAcnTaEwDQYJKoZIhvCNQEFBQAwdTELMAkGA1UEBhMCVVMxGDAWBgNV
[...]
KoZIhvCNQEBBQAEgYCofks852BV77NVuw53vSx01XtI2JhC1CDlu+tcTPoMD1wq5dc5v40
Tgsaw0N8dqgVLk8aC/CdGMbRBu+J1LKrcVza+khnjjtB66HhDRLrjmEGDNttrEjbqvpd2Q02
vxB3iPTlU+vCGXo47e6GyRydqTpboqr49Zqmx+IJ6Z7iigAAAAAAA==
```

```
-----ms050405070101010502050101--
```

# Assinaturas cegas

- **Assinaturas pode ser efetuadas de forma cega**
  - Assinante não consegue observar os conteúdos assinados
  - Semelhante a assinar um envelope com um documento e um papel químico
- **Servem para garantir o anonimato e a não alteração da informação assinada**
  - O assinante X sabe quem lhe pede a assinatura (Y)
  - X assina  $T_1$ , mas Y depois recupera a assinatura sobre  $T_2$ 
    - $T_2$  não é qualquer, está relacionado com  $T_1$
  - O requerente pode apresentar  $T_2$  assinado por X
    - Mas não pode alterar  $T_2$
    - X não consegue associar  $T_2$  ao  $T_1$  que viu e assinou

# Derivação de Chaves

- **Algoritmos requerem chaves de dimensão fixa**
  - 56, 128, 256... bits
- **Necessário derivar chaves de várias fontes**
  - Segredos partilhados
  - Passwords geradas por humanos
  - Códigos PINs e segredos pequenos..
- **Fonte original pode ter baixa entropia**
  - Reduz dificuldade de um ataque de força bruta
  - Necessário existir uma transformação complexa entre fonte e chave
- **Necessário poder-se chegar a múltiplas chaves para a mesma password**
  - Evitar deduzir a password a partir da chave gerada

# Derivação de Chaves

- **Reforço das chaves: Aumento da segurança de uma password**
  - Tipicamente definida por humanos
  - Tornar os ataques por dicionário impraticáveis
- **Expansão das chaves: Aumento da dimensão de uma password**
  - Expansão até ao pretendido para o algoritmo
  - Eventualmente também a geração de outros valores como chaves para MACs

# Derivação de Chaves

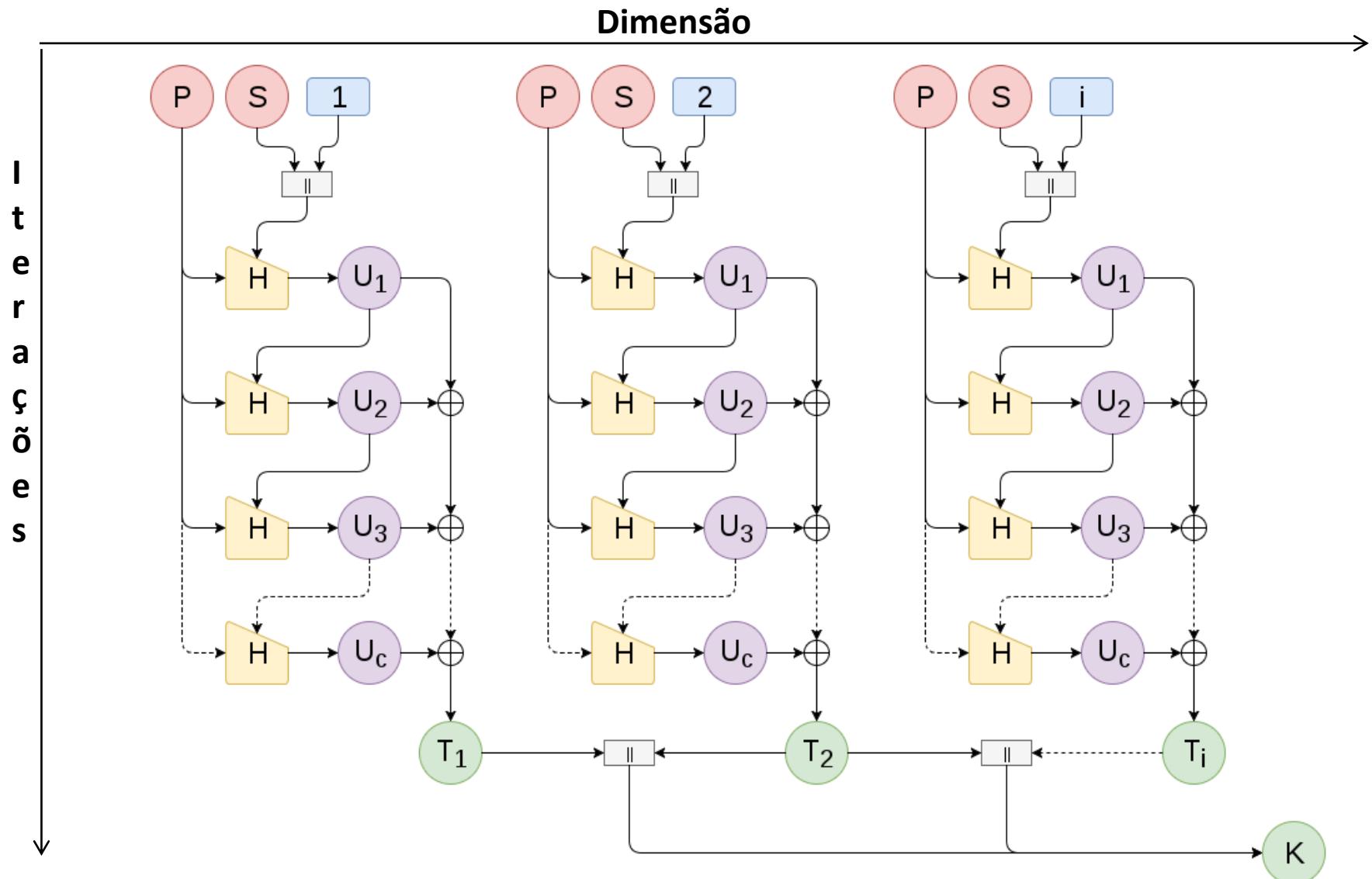
- **Derivação de chaves impõe a existência de:**
  - um Sal que torna a geração única
  - um problema custoso
  - um grau de complexidade parametrizável
- **Dificuldades computacionais:** Transformação requer recursos computacionais relevantes para ser realizada
- **Dificuldades de armazenamento:** Transformação ocupa recursos de armazenamento relevantes (memória)

# Derivação de Chaves: PBKDF2

## Password Based Key Derivation Function 2

- **Produz uma chave com um custo computacional pré-definido**
- **$K = \text{PBKDF2(PRF, Sal, Iterações, Password, dim)}$** 
  - PRF: Pseudo-Random-Function: Uma síntese
  - Sal: Um valor aleatório
  - Iterações: O custo (um valor nas centenas de milhares)
  - Password: Um segredo
  - Dim: a dimensão do resultado pretendido
- **Operação: Realiza  $N \times \text{dim}$  operações do PRF, com base no SAL e password**
  - Quanto maior o valor de N, maior o custo

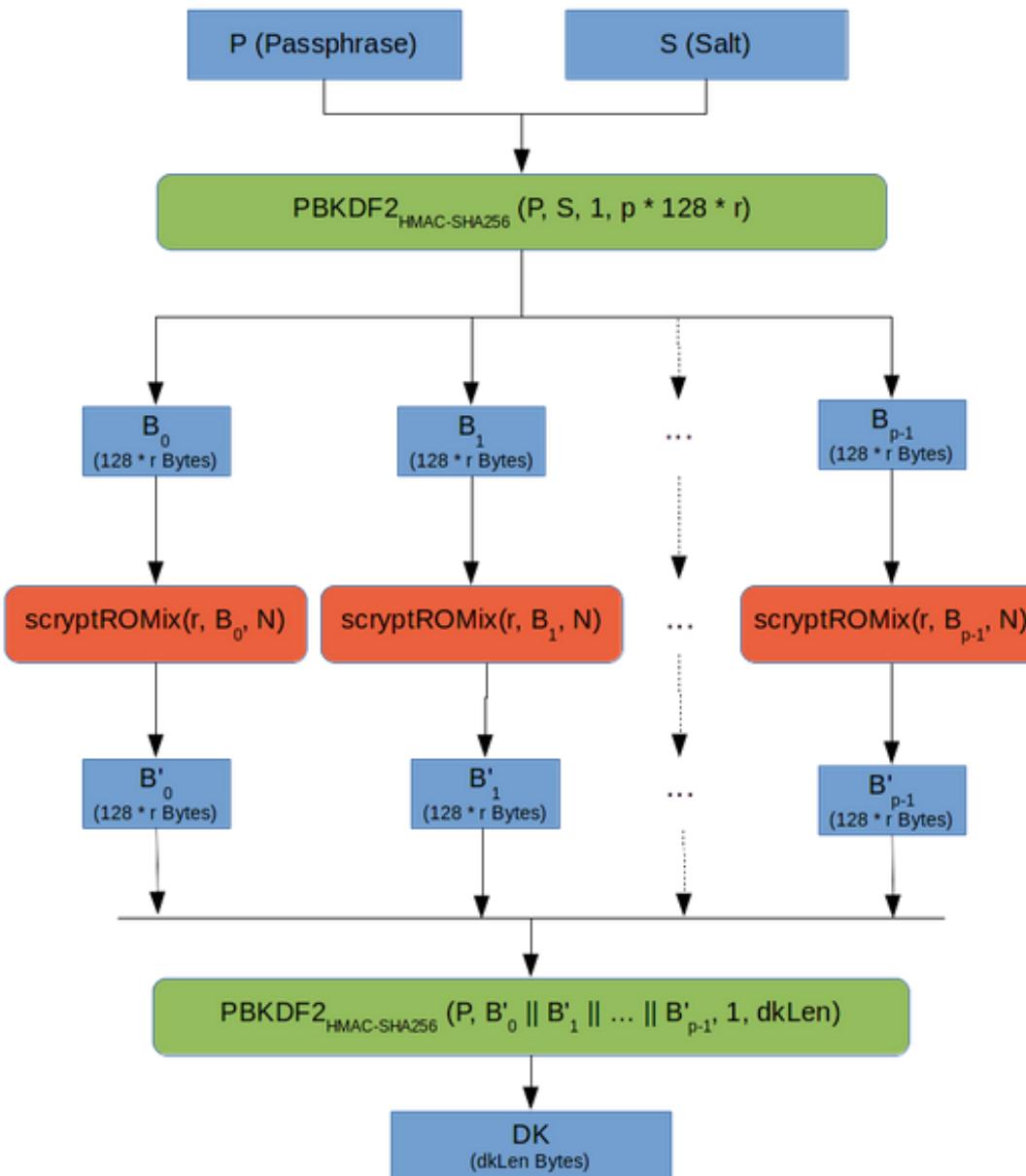
# Derivação de Chaves: PBKDF2



# Derivação de Chaves: scrypt

- Produz uma chave com um custo de armazenamento pré-definido
- $K = \text{scrypt}(\text{Password}, \text{Sal}, N, p, \text{dim}, r, hLen, MLen)$ 
  - Password: um segredo a expandir
  - Sal: Um valor aleatório
  - N: parâmetro de custo
  - p: Parâmetro de paralelização.  $p \leq (2^{32}-1) * hLen / MLen$
  - dim: a dimensão da chave a produzir
  - r: o tamanho dos blocos a usar (tipicamente 8)
  - hLen: dimensão da função de síntese (32 para SHA256)
  - MLen: bytes na mistura interna (tipicamente  $8 \times r$ )

# Derivação de Chaves: scrypt



# Gestão de Chaves Assimétricas

# Problemas a resolver

## **Garantir a utilização apropriada dos pares de chaves**

- **Privacidade das Chaves Privadas**
  - Para garantir autenticidade
  - Para prevenir a repudiação das assinaturas
- **Distribuição correta das chaves públicas**
  - Para garantir confidencialidade
  - Para garantir a validação correta das assinaturas digitais

# Problemas a resolver

**Evolução temporal do mapeamento entre  
entidade<->par de chaves**

- **Lidar com ocorrências catastróficas**
  - Perda de chave privada
- **Lidar com requisitos básicos da sua exploração**
  - Atualizar pares para reduzir riscos de impersonificação

# Problemas a resolver

## **Garantir a geração correta dos pares de chaves**

- **Garantir uma qualidade dos pares de chave**
  - Aleatoriedade do gerador dos valores secretos
  - Evitar que possam ser adivinhados
- **Melhorias da eficiência sem comprometer a segurança**
  - Tornar os mecanismos mais úteis
  - Aumentar a performance

# Objetivos

## 1. Geração de pares de chaves

- Quando e como devem ser gerados

## 2. Manuseamento de chaves privadas

- Como manter privadas

## 3. Distribuição de chaves públicas

- Como devem ser distribuídas para todo o mundo

## 4. Ciclo de vida dos pares de chaves

- Qual a sua expiração
- Como podem ser utilizadas
- Como verificar a sua obsolescência

# Geração de Chaves: Princípios

## Utilizar geradores bons na produção de segredos

- **Resultado é indistinguível de ruído**
  - Todos os valores possuem probabilidade igual
  - Não existem padrões derivados no número da iteração ou valores anteriores
- **Exemplo: Gerador de Bernoulli**
  - Gerador sem memória
  - $P(b=1) = P(b=0) = 1/2$
  - Igual a atirar ao ar uma moeda perfeita

# Geração de Chaves: Princípios

**Facilitar os processos sem comprometer a segurança**

- **Chaves públicas eficientes**
  - Dimensão reduzida, tipicamente valores  $2^k+1$ 
    - ex 3, 17, 65537
  - Acelera operações com chaves públicas
  - Não adiciona questões de segurança

# Geração de Chaves: Princípios

**A chave privada deve ser *gerada pelo próprio***

- **Para assegurar ao máximo a sua privacidade**
  - Apenas o seu dono possui a chave
  - Melhor: O dono também não ter a chave, apenas acesso aos processos com ela
- **Este princípio pode ser relaxado se não se pretender assinaturas digitais**
  - Onde não existem questões relacionadas com não repudiação

# Geração de Chaves: Cuidados

## Correção

- **A chave privada representa um sujeito**
  - ex: um cidadão
  - O risco do seu comprometimento deve ser minimizado
  - Considerar igualmente cópias de salvaguarda
- **O caminho de acesso à chave deve ser controlado**
  - Correção das aplicações que a usam
  - Utilização de autenticação nas aplicações
  - Cifra da chave privada

# Geração de Chaves: Cuidados

## Confinamento

- **Armazenamento da chave numa entidade autónoma segura**
  - Módulo seguro de hardware interno
  - Partição lógica segura a nível do CPU
  - Smartcard ou chave externa
- **Utilização protegida da chave**
  - Aplicações não utilizam a chave
  - Invoca-se ao dispositivo a realização de operações

# Distribuição de Chaves Públicas

**Problema: Como distribuir uma chave pública ao mundo?**

- **Distribuição a quem pretenda enviar informação confidencial**
  - manual
  - protegida por um segredo partilhado
  - de forma Ad-hoc usando certificados digitais
- **Distribuição a quem pretenda validar informação autenticada**
  - manual
  - de forma Ad-hoc usando certificados digitais

# Distribuição de Chaves Públicas

**Problema: Como garantir a correção de uma chave pública?**

- **Disseminação confiável de chaves públicas**
  - Usar caminhos ou grafos de relações de confiança

**Se A confia em  $K_x+$ , e B confia em A,**

**então B confia em  $K_x+$**

- **Hierarquias e grafos de certificação**
  - Expressão clara das relações de confiança entre entidades
  - Certificação é unidirecional

# Certificados Digitais de Chaves Públicas

**Documentos digitais emitidos por uma Entidade Certificadora (EC)/Certification Authority (CA)**

- **Ligam uma chave pública a uma entidade**
  - Pessoa, sistema ou serviço
- **São documentos públicos**
  - Contém apenas informação pública
  - Podem contém informação adicional associada à entidade
- **São seguros por meios criptográficos**
  - Possuem uma impressão digital para identificação
  - São assinados com uma assinatura digital criada pelo emissor (CA)

# Certificados Digitais de Chaves Públicas

**Usados para distribuir chaves públicas de forma confiável**

- **Os verificadores podem validar os documentos**
  - Validar identificação com o contexto atual
  - Validar instantes temporais
  - Validar a utilização da chave pública
  - Validam a assinatura digital do documento usando a chave pública da CA
- **Os verificadores confiam no comportamento das CA**
  - Portanto confiam nos documentos que emitem
  - Uma CA associou uma chave pública a A. Se o verificador confiar na CA, irá confiar que a associação de A é correta.

# Certificados Digitais de Chaves Públicas

- **Norma X.509v3**
  - Campos obrigatórios
    - Versão
    - Sujeito (subject)
    - Chave pública
    - Datas (início e expiração)
    - Emissor (issuer)
    - Assinatura
    - ...
  - Extensões: definem utilização
    - Críticas ou não Críticas
- **PKCS #6**
  - Extended-Certificate Syntax Standard
- **Formatos binários**
  - ASN.1 (Abstract Syntax Notation)
    - DER, CER, BER, etc.
- **PKCS #7**
  - Cryptographic Message Syntax Standard
- **PKCS #12**
  - Personal Information Exchange Syntax Standard
- **Outros formatos**
  - PEM (Privacy Enhanced Email)
    - Base64

# Utilizações de um par de chaves

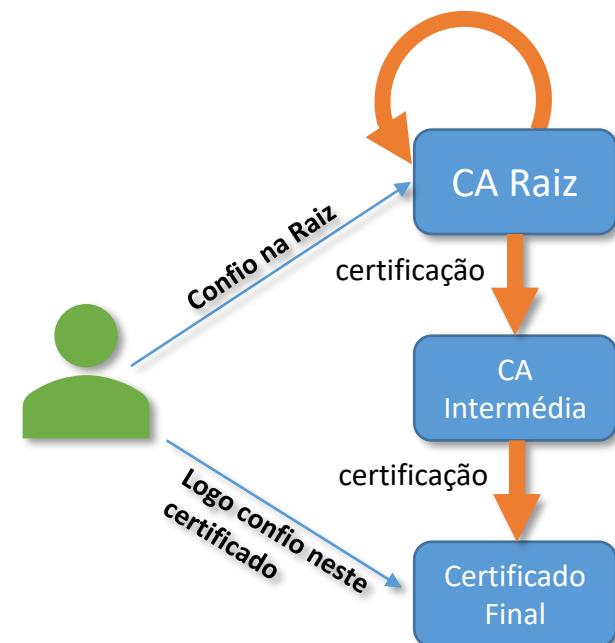
- O certificado associa um par de chaves a um perfil de utilização restrito
  - Uma entidade terá vários certificados, um para cada utilização
  - Definido no certificado, extensão crítica: **Key Usage**
- **Perfis típicos**
  - Autenticação/Distribuição de chaves
    - Assinaturas digitais, Cifra de Chaves, Cifra de Dados, Negociação de chaves
  - Assinatura de documentos
    - Assinaturas digitais, Não-repudiação
  - Emissão de certificados
    - Assinaturas de certificados e objetos relacionados

# Entidades Certificadoras (CA)

- **Organizações que gerem certificados de chave pública**
  - Empresas, entidades sem fins lucrativos ou governamentais
  - Normalmente possuem a tarefa de validar associações chave-entidade
- **Importante que operem corretamente para serem confiáveis**
  - Definem políticas e mecanismos para
  - Emissão de certificados
  - Revogação de certificados
  - Distribuição de certificados
  - Emitir e distribuir as chaves privadas correspondentes
- **Gerem processos de revogação de certificados**
  - Listas de identificadores de certificados revogados
  - Interfaces para verificação do estado do certificado

# Entidades Certificadoras Confiáveis

- **Entidades certificadoras raíz.**
  - Podem ser confiáveis por um grupo restrito, ou uma maioria
  - Possuem processos de gestão confiáveis
- **Entidades certificadoras intermédias: Certificadas por outra CA**
  - Usando um certificado
  - Formam hierarquias de certificação
- **Raízes de confiança ou raízes de certificação**
  - Alguém possui e confia numa chave pública
  - Certificados das CAs são auto assinadas
    - Podem também ser assinados por outras CAs
  - Distribuição Manual
    - nos browsers, no SO



[General](#) [Details](#)**This certificate has been verified for the following uses:**

SSL Client Certificate

SSL Server Certificate

**Issued To**

Common Name (CN) www.ua.pt  
Organization (O) Universidade de Aveiro  
Organizational Unit (OU) sTIC  
Serial Number 06:B4:17:0C:D7:EF:AC:9F:A3:79:9A:78:0E:7E:5A:8C

**Issued By**

Common Name (CN) TERENA SSL CA 3  
Organization (O) TERENA  
Organizational Unit (OU) <Not Part Of Certificate>

**Period of Validity**

Begins On May 27, 2019  
Expires On June 3, 2021

**Fingerprints**

SHA-256 Fingerprint 6C:BA:BD:A1:7E:A9:8D:EA:7B:18:22:44:EC:71:D5:41:4D:08:D  
4:A6:FC:48:1B:3C:9B:05:EB:DA:69:A6:A5:EE  
SHA1 Fingerprint 17:79:15:B5:0E:E0:34:51:2D:FA:DE:DF:77:1E:E1:0A:B3:4B:2F:2B

[Close](#)

General Details**Certificate Hierarchy**

▼ DigiCert Assured ID Root CA

▼ TERENA SSL CA 3

www.ua.pt

**Certificate Fields**

▼ www.ua.pt

▼ Certificate

Version

Serial Number

Certificate Signature Algorithm

Issuer

&gt; Validity

Subject

▼ Subject Public Key Info

Subject Public Key Algorithm

Subject Public Key

**Field Value**

CN = www.ua.pt

OU = sTIC

O = Universidade de Aveiro

L = Aveiro

C = PT

**Export...****Close**

## Certificate Viewer: "TERENA SSL CA 3"

General Details

**This certificate has been verified for the following uses:**

SSL Certificate Authority

### **Issued To**

Common Name (CN) TERENA SSL CA 3  
Organization (O) TERENA  
Organizational Unit (OU) <Not Part Of Certificate>  
Serial Number 08:70:BC:C5:AF:3F:DB:95:9A:91:CB:6A:EE:EF:E4:65

### **Issued By**

Common Name (CN) DigiCert Assured ID Root CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com

### **Period of Validity**

Begins On November 18, 2014  
Expires On November 18, 2024

### **Fingerprints**

SHA-256 Fingerprint BE:B8:EF:E9:B1:A7:3C:84:1B:37:5A:90:E5:FF:F8:04:88:48:E3:  
A2:AF:66:F6:C4:DD:7B:93:8D:6F:E8:C5:D8  
SHA1 Fingerprint 77:B9:9B:B2:BD:75:22:E1:7E:C0:99:EA:71:77:51:6F:27:78:7C:AD

Close

## Certificate Viewer: "TERENA SSL CA 3"

General Details

This certificate has been verified for the following uses:

SSL Certificate Authority

### Issued To

Common Name (CN) TERENA SSL CA 3  
Organization (O) TERENA  
Organizational Unit (OU) <Not Part Of Certificate>  
Serial Number 08:70:BC:C5:AF:3F:DB:95:9A:91:CB:6A:EE:EF:E4:65

### Issued By

Common Name (CN) DigiCert Assured ID Root CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com

### Period of Validity

Begins On November 18, 2014  
Expires On November 18, 2024

### Fingerprints

SHA-256 Fingerprint BE:B8:EF:E9:B1:A7:3C:84:1B:37:5A:90:E5:FF:F8:04:88:48:E3:  
A2:AF:66:F6:C4:DD:7B:93:8D:6F:E8:C5:D8  
SHA1 Fingerprint 77:B9:9B:B2:BD:75:22:E1:7E:C0:99:EA:71:77:51:6F:27:78:7C:AD

CA Intermédia

(Certificado de CA  
emitido por outra CA)

Close

## Certificate Viewer: "DigiCert Assured ID Root CA"

General Details

This certificate has been verified for the following uses:

SSL Certificate Authority

### Issued To

Common Name (CN) DigiCert Assured ID Root CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com  
Serial Number 0C:E7:E0:E5:17:D8:46:FE:8F:E5:60:FC:1B:F0:30:39

### Issued By

Common Name (CN) DigiCert Assured ID Root CA  
Organization (O) DigiCert Inc  
Organizational Unit (OU) www.digicert.com

### Period of Validity

Begins On November 10, 2006  
Expires On November 10, 2031

### Fingerprints

SHA-256 Fingerprint 3E:90:99:B5:01:5E:8F:48:6C:00:BC:EA:9D:11:1E:E7:21:FA:BA:  
35:5A:89:BC:F1:DF:69:56:1E:3D:C6:32:5C  
SHA1 Fingerprint 05:63:B8:63:0D:62:D7:5A:BB:C8:AB:1E:4B:DF:B5:A8:99:B2:4D:43

Close

CA Raiz

(Certificado Auto-emitido)

# Hierarquias de Certificação: Modelo PEM

- **Distribuição de certificados para o Privacy-enhanced Electronic Mail**
- **PEM: Privacy-enhanced Electronic Email**
  - Proposto pelo IETF em 1993 (ERF1421-1423)
- **Modelo de Monopólio**
  - Uma raiz única: IPRA (Internet Policy Registration Authority)
  - Várias PCA (Policy Creation Authorities) abaixo da raiz
  - Várias CAs abaixo de cada PCA
    - Possivelmente pertencentes a organizações e empresas
  - Forma uma cadeira de certificação
  - Árvore de raiz única

# Hierarquias de Certificação: Modelo PEM

- **Modelo nunca foi implementado globalmente**
  - Exceto pequenas implementações (90s)
- **Preferido: Floresta de hierarquias em cada CA, sem uma IPRA**
  - Hierarquias independentes sem uma raiz única
  - Oligarquia
- **Cada CA raiz negocia a distribuição da sua chave pública em cada entidade**
  - Entidade: Browsers, Distribuições, Sistemas, Sistema Operativos

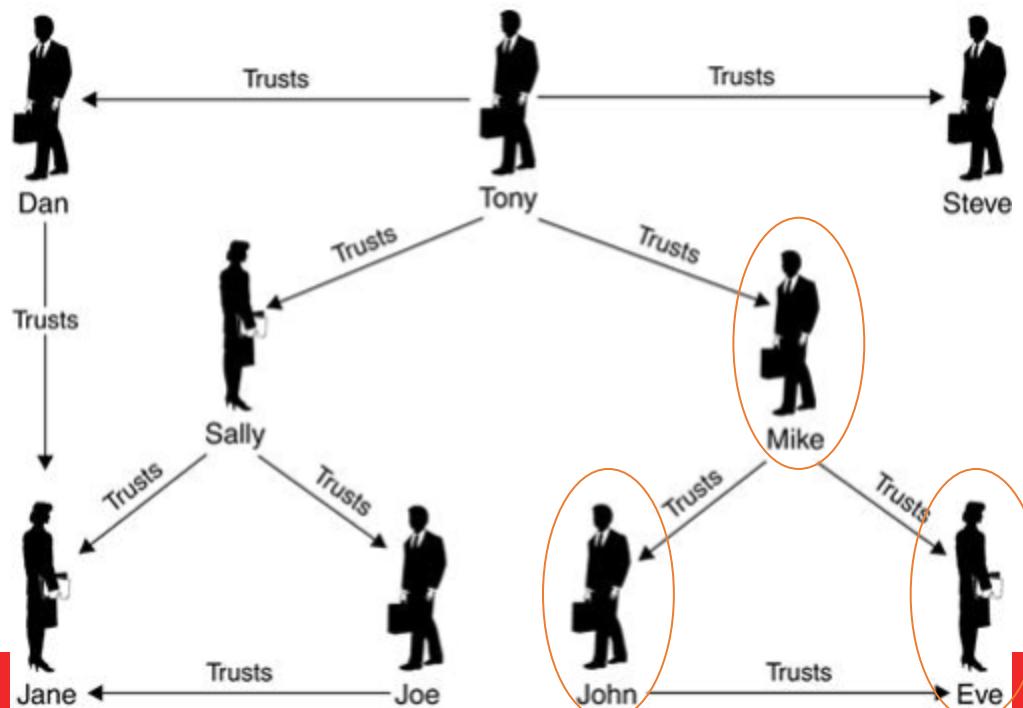
# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

- **Segue um modelo baseado numa rede de confiança**
  - E não numa árvore
- **Sem qualquer autoridade central de confiança**
  - Qualquer pessoa/entidade é um potencial certificador
  - Qualquer pessoa/entidade pode certificar uma chave pública e publicar a assinatura para os outros
- **Pessoas usam dois tipos de confiança**
  - Confiança nas chaves que conhecem
    - Validadas diretamente por qualquer meio (presença, telefone,...)
  - Confiança no comportamento de outros certificadores
    - Assumindo que verificam as chaves que certificam

# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

## Confiança Transitiva

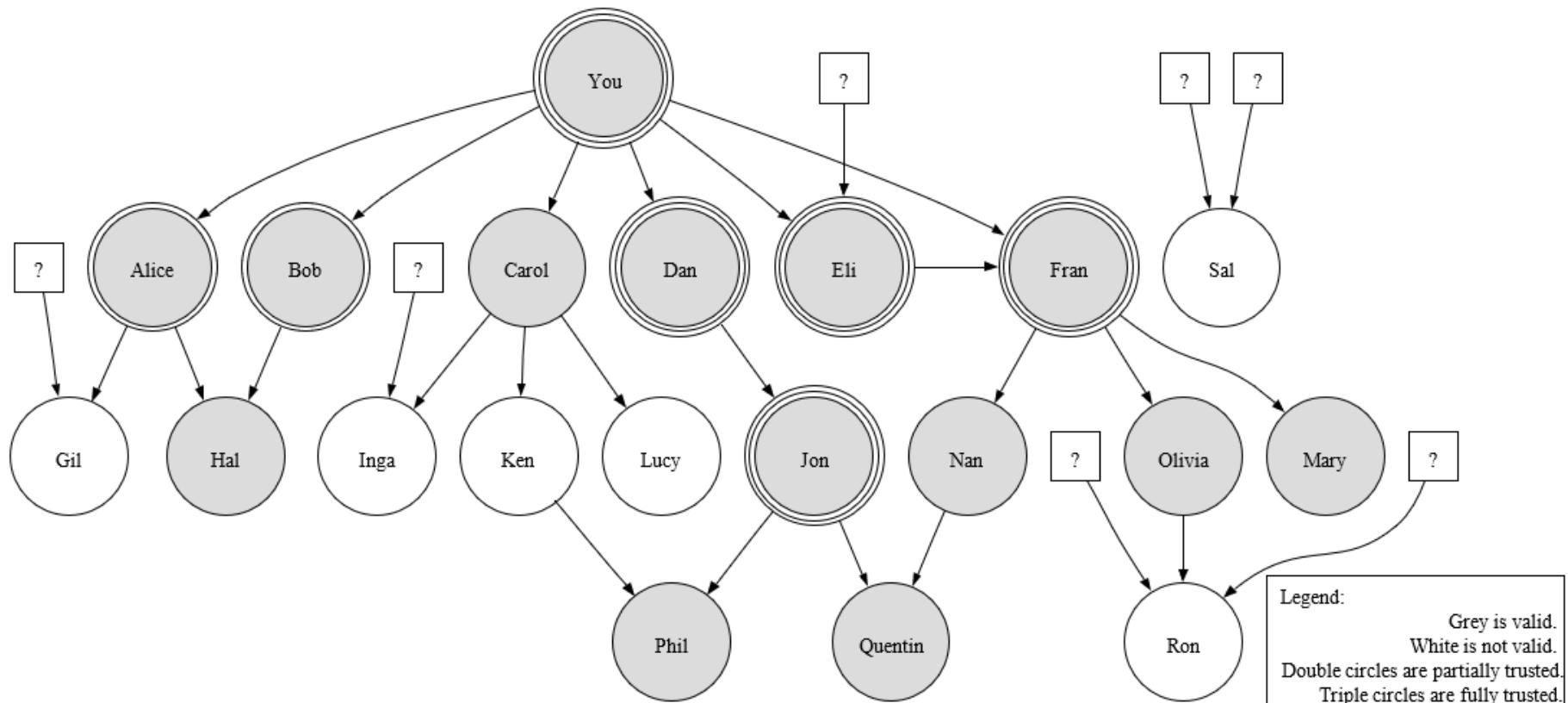
1. SE Mike confia que o John é um certificador correto,
2. E John certificou a chave pública de Eve,
3. ENTÃO Mike confia na chave pública de Eve



# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)

- **Confiança:** Quando uma pessoa confia noutra pessoa
  - Confiança é unidirecional, pessoal e subjetiva
  - Níveis:
    - Ultimate: chaves próprias das quais se tem a chave privada
    - Complete
    - Marginal
    - NoTrust (ou Untrusted)
- **Validade:** Quanta verificação a chave possui (ex, de E perante A)
  - Válida:
    - A confia completamente em B, ou A confia marginalmente em C e D
    - e D ou B em conjunto com C assinaram a chave de E
  - Marginalmente Válida:
    - A confia marginalmente em B e B assinou a chave de E
  - Inválida: sem um caminho

# Hierarquias de Certificação: Modelo PGP (Pretty Good Privacy)



# Refrescamento de chaves assimétricas

- **Pares de chaves devem ter uma validade limitada**
  - Porque as chaves privadas podem ser perdidas ou descobertas
  - Para implementar mecanismos de atualização periódicos
- **Problemas:**
  - Os certificados podem ser copiados e distribuídos livremente
  - O universo de possuidores de certificados é desconhecido
    - Não é viável contactar todos os possuidores de certificados para eliminar certificados específicos
- **Soluções:**
  - Certificados com uma validade temporal definida (não antes, não depois)
  - Listas de Revogação de Certificados (CRL)
    - Para permitir revogar certificados antes que expirem

# Listas de Revogação de Certificados (CRL)

- **Listas assinadas com identificadores de certificados revogados prematuramente**

- Devem ser consultadas periodicamente pelos verificadores
- Entradas podem conter a razão



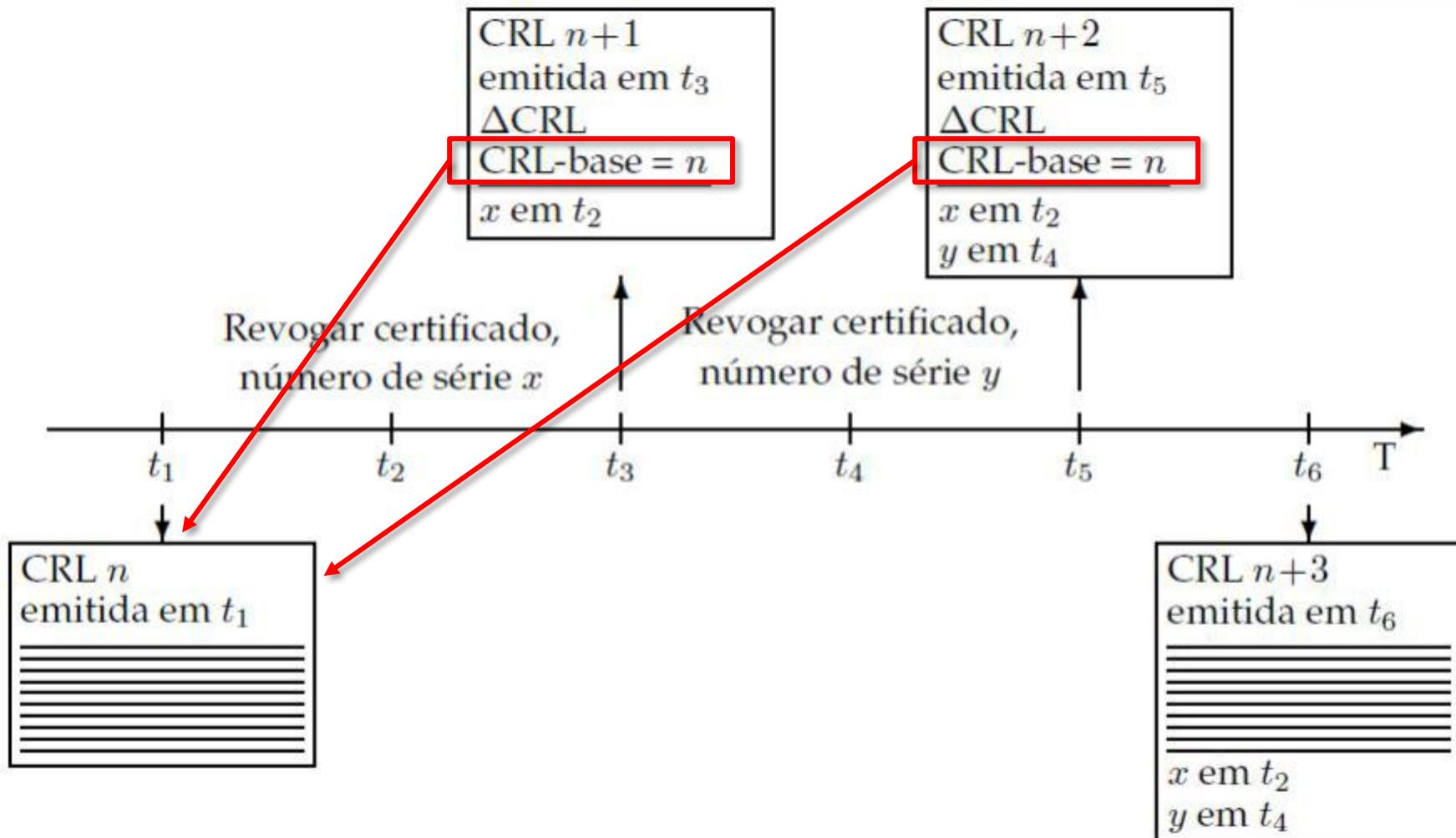
- **Publicação e distribuição de CRLs**

- Cada CA possui a sua CRL
- De acesso público
- CAs trocam CRLs para facilitar distribuição

- **Vários formatos disponíveis**

- Base CRL: Lista completa com todos os certificados revogados
- Delta CRL: Lista com as diferenças desde a última Base CRL
- OCSP: API para verificação individual de cada certificado

# Base CRL, Delta CRL e Revogação



# Online Certificate Status Protocol

- **Protocolo baseado em HTTP para verificar a revogação de certificados**
  - Pedido inclui o número de série do certificado
  - Resposta assinada pela CA afirma qual o estado
  - Uma verificação por certificado
- **Reduz a largura de banda usada pelos clientes**
  - Um pedido por certificado, em vez de toda a lista (Base CRL)
- **Pode envolver maior largura de banda para as CAs**
  - Se clientes validarem sempre os certificados
  - Pode comprometer a privacidade. CA sabe quando um sistema acede a um serviço
- **OCSP Stapling**
  - Inclui um instante temporal assinado na resposta
  - Clientes podem guardar respostas durante a sua validade

# Distribuição de certificados de chave pública

- **Transparente e integrado nos sistemas e aplicações**
  - Sistemas de Diretórios
    - Grandes escala: usando X.500 através de LDAP
    - Organizações: Windows Active Directory, Manualmente
  - Online: incluído nos protocolos
    - comunicações seguras usando TLS
    - Assinaturas digitais de correio com MIME ou em documentos
  - Pré-distribuição
    - Incluído nas aplicações, Sistemas Operativos
- **Explicitamente pelos utilizadores**
  - Utilizador pede um certificado específico
  - Por email, acesso a uma página HTTP

# PKI: Public Key Infrastructure

**Infraestrutura de apoio ao uso de pares de chaves e certificados**

- **Criação segura de pares de chaves assimétricas**
  - Políticas de subscrição
  - Políticas de geração de pares de chaves
- **Criação e distribuição de certificados de chaves públicas**
  - Políticas de subscrição
  - Definição de atributos do certificado

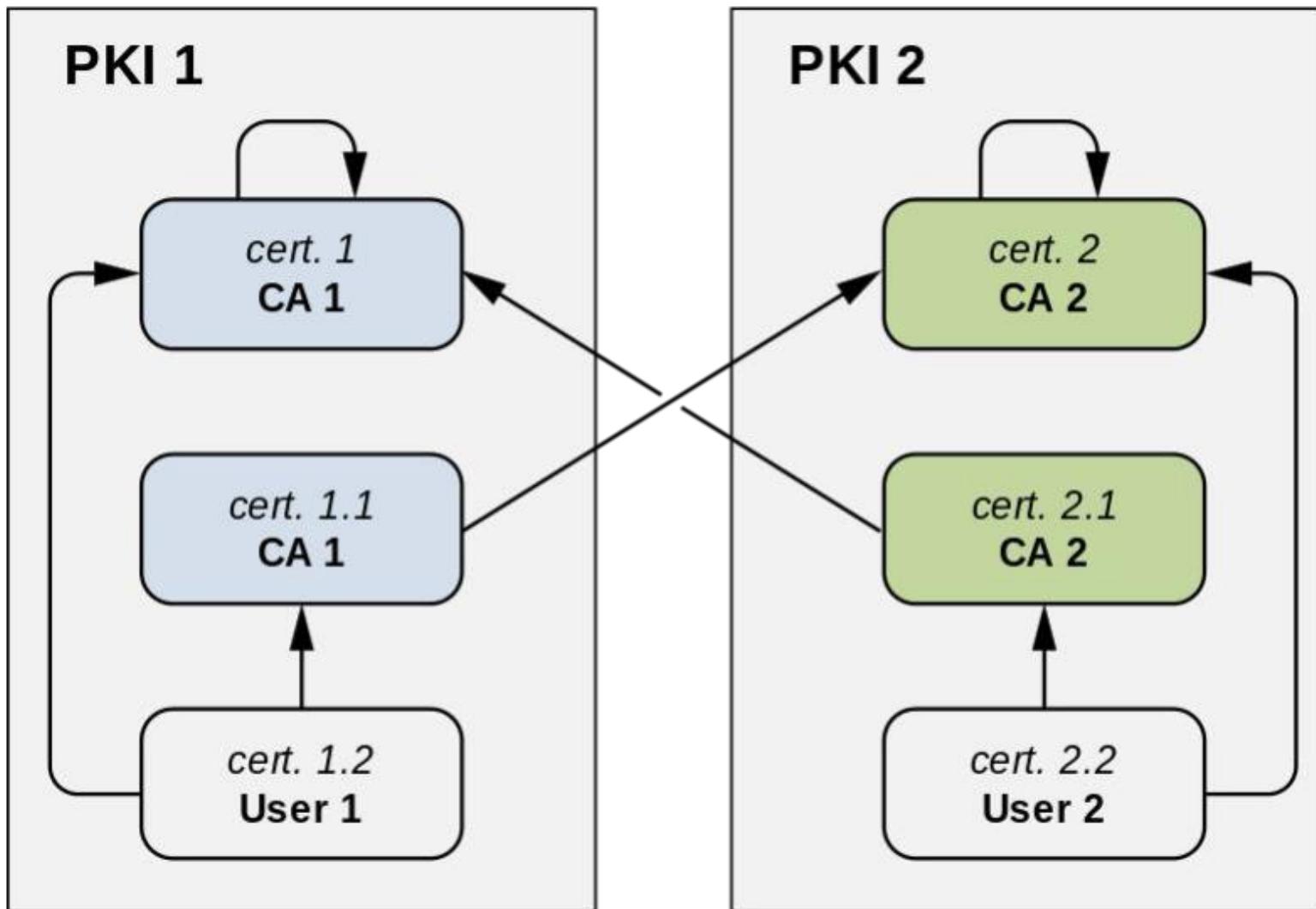
# PKI: Public Key Infrastructure

- **Definição e uso de cadeias de certificação**
  - Inserção numa hierarquia de certificação
  - Certificação de outras Cas
- **Atualização, publicação e consulta de listas de certificados revogados**
  - Políticas para revogar certificados
  - Distribuição permanente de CRLs
  - Serviço OCSP
- **Uso de estruturas de dados e protocolos que permitem a interoperação entre componentes**

# PKI: Relações de Confiança

- Um PKI estabelece relações de confiança de duas formas
  - Emitindo certificados de chaves públicas de outras CAs
    - Abaixo na hierarquia; ou
    - Não relacionadas hierarquicamente
  - Requerendo a certificação da sua chave pública a outras CAs
    - Acima na hierarquia; ou
    - Não relacionadas hierarquicamente
- Relações de confiança características
  - Hierárquicas
  - Cruzadas (A certifica B e vice-versa)
  - Ad-hoc (meshed)
    - Grafos mais ou menos complexos de certificação

# PKI: Certificação Hierárquica e Cruzada



# PKI: Fixação dos Certificados (Pinning)

- Se um atacante possui acesso a uma raiz de confiança, ele pode emitir qualquer certificado para qualquer entidade
  - Manipular a CA para que ela emita um certificado (difícil)
  - Injetar raízes adicionais nos sistemas da vítima (mais fácil)
- **Certificate Pinning:** Adicionar uma impressão digital da chave pública **ao código**
  - Impressão Digital usa uma síntese (e.x, SHA256)
  - Associada a um pedido HTTP específico
- **Processo de validação normal + verificação de impressão digital**
  - Certificado tem de ser assinado por uma raiz de confiança
  - Certificado tem de ter uma chave pública com a impressão digital especificada

# Transparência de Certificação (RFC 6962)

- **Problemas**

- CAs podem ser comprometidas (Ex, DigiNotar)
  - Por atacantes maliciosos
  - Por governos, etc...
- Comprometimento é difícil de detetar
  - Resulta na alteração das regras de funcionamento da PKI
  - Dono legítimo dificilmente saberá

- **Definição: Sistema que regista todos os certificados públicos emitidos**

- Garante que só são publicados certificados que levam a raízes legítimas
- Armazena toda a cadeia de certificação de cada certificado
- Apresenta esta informação para auditoria
  - Organizações ou ad-hoc pelos utilizadores