ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

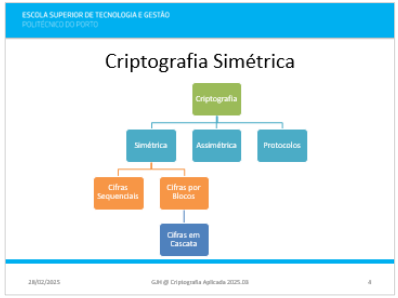
P.PORTO

Criptografia Aplicada

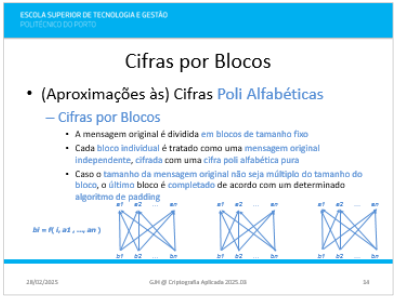
Criptografia Simétrica

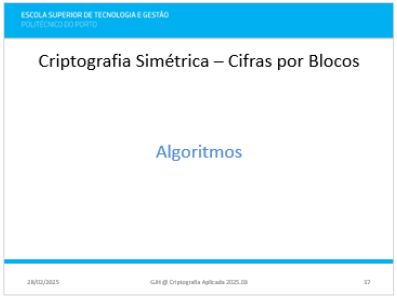
Agenda


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Moderna
Principio de Kerchoff
A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.
Nos primórdios da criptografia, considerava-se que a segurança deveria ser mantida através do obscurantismo, mantendo a confidencialidade dos algoritmos utilizados, com várias desvantagens:
Ao reduzir o número de pessoas que conheciam o algoritmo, limitava-se também o número de pessoas que poderia identificar os seus pontos fracos
A presunção de que o algoritmo é desconhecido de potenciais atacantes reduz o incentivo para procurar elevados níveis de segurança
Assim, com a criptografia moderna ganhou proeminência a corrente de opinião inerente ao principio de Kerchoff, segundo o qual os algoritmos devem ser públicos e apenas as chaves secretas
28/02/2025
GJH @ Criptografia Aplicada 2025.03
3


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Simétrica
Criptografia
Simétrica
Assimétrica
Protocolos
Cifras Sequenciais
Cifras por Blocos
Cifras em Cascata
28/02/2025
GJH @ Criptografia Aplicada 2025.03
4

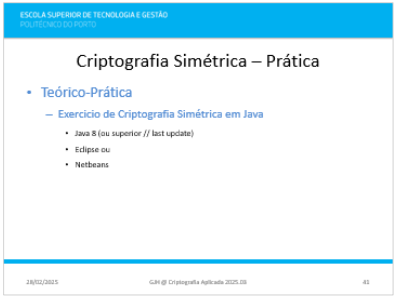

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Cifras Sequenciais
(Aproximações às) Cifras Poli Alfabéticas
Cifras Sequenciais
Seguem o mesmo princípio dos one-time pads mas em que cada símbolo ki da chave utilizada é calculado por um gerador de chaves, a partir do seu estado actual (ei) e dos anteriores símbolos cifrados (ax) e símbolos da chave (kx)
A chave de cifra é o estado inicial (e0) do gerador de chaves
São mais apropriadas para a cifragem de mensagens em tempo real e, ao contrário dos one-time pads, permitem cifrar mensagens de tamanho ilimitado
28/02/2025
GJH @ Criptografia Aplicada 2025.03
6


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Cifras por Blocos
(Aproximações às) Cifras Poli Alfabéticas
Cifras por Blocos
A mensagem original é dividida em blocos de tamanho fixo
Cada bloco individual é tratado como uma mensagem original independente, cifrada com uma cifra poli alfabética pura
Caso o tamanho da mensagem original não seja múltiplo do tamanho do bloco, o último bloco é completado de acordo com um determinado algoritmo de padding
28/02/2025
GJH @ Criptografia Aplicada 2025.03
14


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Simétrica – Cifras por Blocos
Algoritmos
28/02/2025
GJH @ Criptografia Aplicada 2025.03
17


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Simétrica – Cifras por Blocos
Modo de Operação
28/02/2025
GJH @ Criptografia Aplicada 2025.03
23

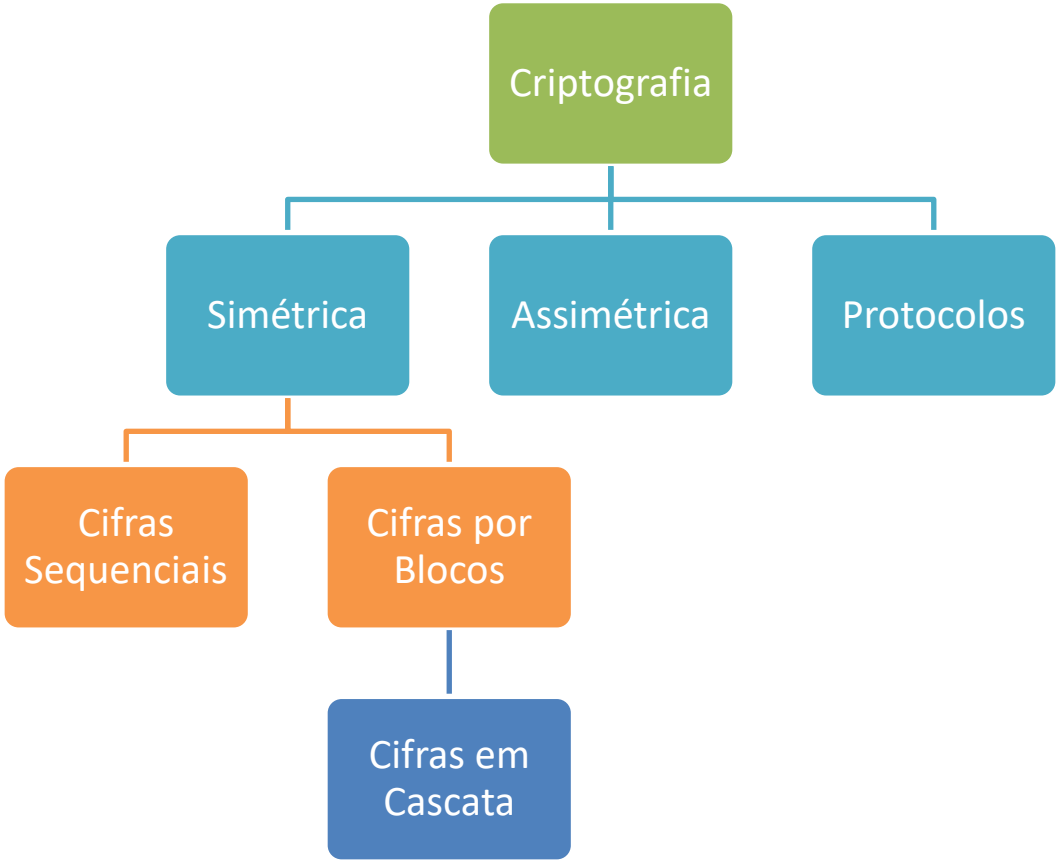

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Simétrica – Cifras por Blocos
Padding
28/02/2025
GJH @ Criptografia Aplicada 2025.03
34


ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO
Criptografia Simétrica – Prática
Teórico-Prática
Exercicio de Criptografia Simétrica em Java
Java 8 (ou superior // last update)
Eclipse ou
Netbeans
28/02/2025
GJH @ Criptografia Aplicada 2025.03
41

Criptografia Moderna

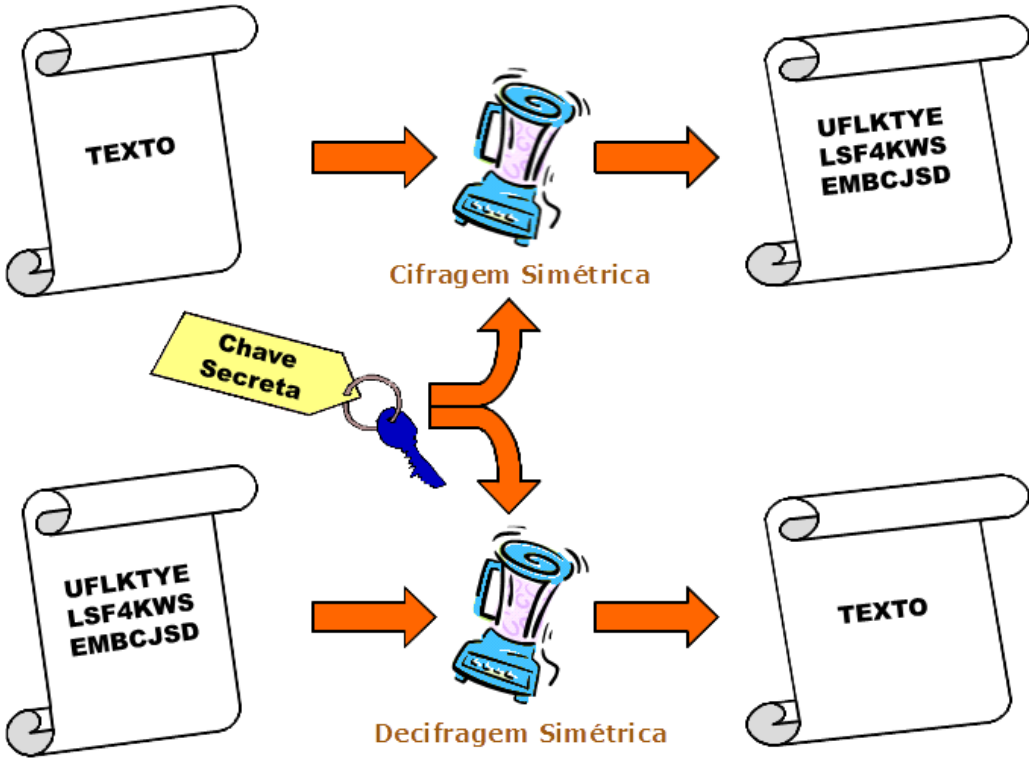
- Principio de Kerchoff
  - *A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.*
  - Nos primórdios da criptografia, considerava-se que a segurança deveria ser mantida através do obscurantismo, mantendo a confidencialidade dos algoritmos utilizados, com várias desvantagens:
    - Ao reduzir o número de pessoas que conheciam o algoritmo, limitava-se também o número de pessoas que poderia identificar os seus pontos fracos
    - A presunção de que o algoritmo é desconhecido de potenciais atacantes reduz o incentivo para procurar elevados níveis de segurança
  - Assim, com a criptografia moderna ganhou proeminência a corrente de opinião inerente ao princípio de Kerchoff, segundo o qual os algoritmos devem ser públicos e apenas as chaves secretas

Criptografia Simétrica



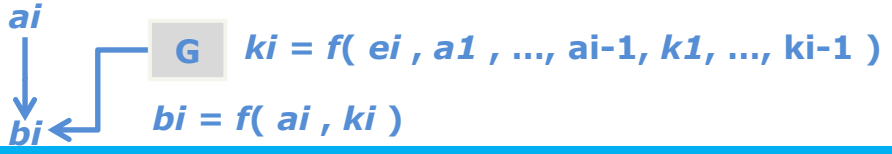
Criptografia Simétrica

- Funcionamento



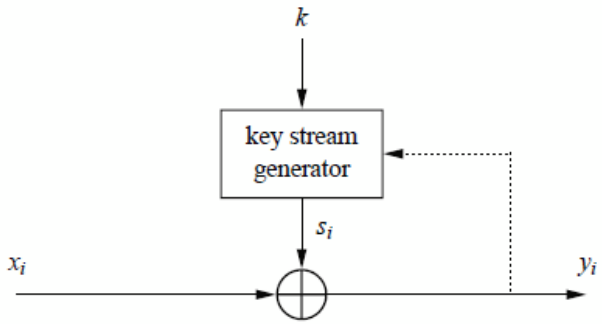
Cifras Sequenciais

- (Aproximações às) Cifras Poli Alfabéticas
  - Cifras Sequenciais
    - Seguem o mesmo princípio dos one-time pads mas em que cada símbolo ki da chave utilizada é calculado por um gerador de chaves, a partir do seu estado actual (ei) e dos anteriores símbolos cifrados (ax) e símbolos da chave (kx)
    - A chave de cifra é o estado inicial (e0) do gerador de chaves
    - São mais apropriadas para a cifragem de mensagens em tempo real e, ao contrário dos one-time pads, permitem cifrar mensagens de tamanho ilimitado



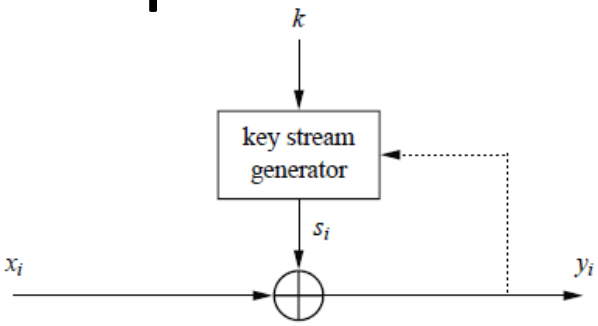
Criptografia Simétrica - Cifras Sequenciais

- Cifras Sequenciais (ou Stream Ciphers)
  - Encriptam bits individualmente
  - Operação baseada no modulo 2:
    - Resultado é sempre 0 ou 1
    - Cifra: yi = Csi (xi) ≡ xi+si mod 2
    - Decifra: xi = Dsi (yi) ≡ yi+si mod 2
  - Utiliza-se XOR para implementar mod 2



x_i	s_i	$y_i \equiv x_i + s_i \bmod 2$
0	0	0
0	1	1
1	0	1
1	1	0

Criptografia Simétrica - Cifras Sequenciais



- Cifras Sequenciais (ou Stream Ciphers)

Podem ser classificadas de acordo com o gerador de chaves:

- Síncronas
  - O gerador de chaves é uma máquina de estados determinista, pelo que o estado inicial e0 determina completamente a sequência de chaves
  - São simples de implementar mas exigem mecanismos auxiliares para manter o sincronismo entre cifragem e decifragem
- Auto Sincronizáveis (ou Assíncronas)
  - Chaves são geradas apenas em função de um subconjunto dos símbolos já cifrados, não dependendo das chaves anteriores
  - Não carecem de sincronização externa mas dificultam a deteção de perdas ou repetições de partes do criptograma

Criptografia Simétrica - Cifras Sequenciais

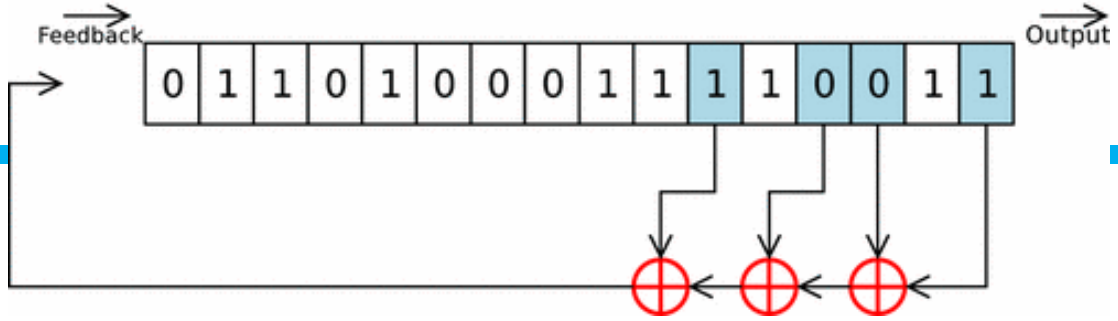
- Cifras Sequenciais - Geradores de números aleatórios (RNG)
  - Segurança conseguida via confiança nas chaves que devem ser aleatórias
  - True Random Number Generators (TRNG)
    - O seu resultado não consegue ser reproduzido
    - Ex: atirar 500x moeda ao ar -> sequencia de 500bits -> replica com sucesso de $\frac{1}{2^{500}} \approx 3{,}0549 * 10^{-151}$
    - Baseados em processos físicos (moeda ao ar, atirar dados, barulho em semicondutor, …)
  - (General) Pseudorandom Number Generators (PRNG)
    - Sequencias geradas a partir de um valor inicial (semente/seed)
    - Não são realmente aleatórios porque podem ser computados (são determinísticos) (ex: rand() na linguagem C)
    - Requisito: propriedades estatísticas elevadas onde resultado é uma sequencia aproximada de TRNG
  - Cryptographically Secure Pseudorandom Number Generators (CSPRNG)
    - Tipo de PRNG imprevisível: a partir de uma sequencia da chave é impossível calcular as sequencias seguintes

Criptografia Simétrica - Cifras Sequenciais

- Cifras Sequenciais

Normalmente implementadas (longas sequências de valores pseudo aleatórios - PRNG) recorrendo a combinações não-lineares de LFSRs (Linear Feedback Shift Registers)

- Estes permitem efetuar shifts binários recursivos de acordo com um determinado polinómio característico
- O processo é controlado pelo valor do seu estado anterior
- A sua implementação em hardware é simples mas, para colmatar as vulnerabilidades inerentes à sua linearidade, devem utilizar-se combinações não lineares dos mesmos



Criptografia Simétrica - Cifras Sequenciais

- Cifras Sequenciais (Algoritmos mais populares)
  - RC4
    - Apesar de inicialmente ser secreto, o seu algoritmo foi descoberto em 1994
    - Utilizado na cifragem de protocolos como o SSL e o WEP, embora a sua utilização já não seja considerada segura
    - Permite chaves entre os 40 e os 2.048 bits
  - SEAL
    - Derivado das técnicas utilizadas nas funções de hash SHA e SHA-1
    - Bastante utilizada para cifrar o conteúdo de discos rígidos, dada a sua enorme eficácia

Criptografia Simétrica - Cifras Sequenciais

- Cifras Sequenciais (Algoritmos mais populares)
  - A5/1 (A5/2, A5/3)
    - Utilizada para comunicações OTA (Over The Air) no standard GSM
    - Apesar de inicialmente ser secreto, o seu algoritmo ficou de conhecimento público devido a fugas de informação (leaks) e reverse engineer
  - Trivium
    - Utiliza chaves de 80 bits
    - Implementações com bom equilíbrio entre velocidade via hardware e eficácia via software

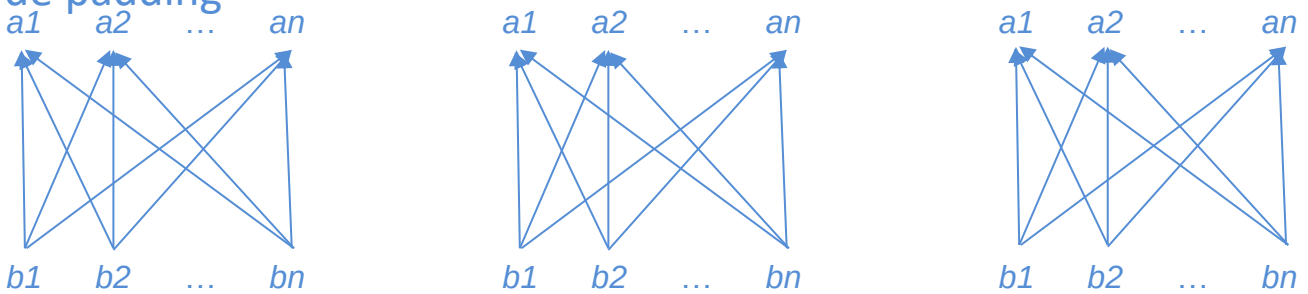
Criptografia Simétrica - Cifras Sequenciais

- Questões?

Cifras por Blocos

- (Aproximações às) Cifras Poli Alfabéticas
  - Cifras por Blocos
    - A mensagem original é dividida em blocos de tamanho fixo
    - Cada bloco individual é tratado como uma mensagem original independente, cifrada com uma cifra poli alfabética pura
    - Caso o tamanho da mensagem original não seja múltiplo do tamanho do bloco, o último bloco é completado de acordo com um determinado algoritmo de padding

$bi = f(i, a1 , ..., an)$



Criptografia Simétrica – Cifras por Blocos

- Cifras por Blocos (Block Ciphers)
  - A mensagem original é dividida em blocos de tamanho fixo
  - Combinação de operações simples (substituições e permutações)
  - Resultado = repetição processo (iterações/rounds)
  - Utilizam chaves derivadas da chave original

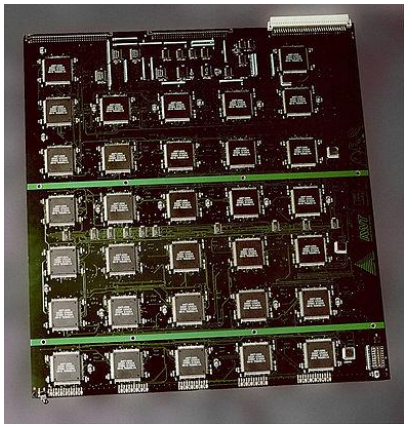
Criptografia Simétrica – Cifras por Blocos

- Cifras por Blocos (Block Ciphers)
  - São implementadas através de
    - Algoritmos específicos aplicados através de um
    - Modo de operação e finalizados através de mecanismos de
    - Padding

Criptografia Simétrica – Cifras por Blocos

Algoritmos

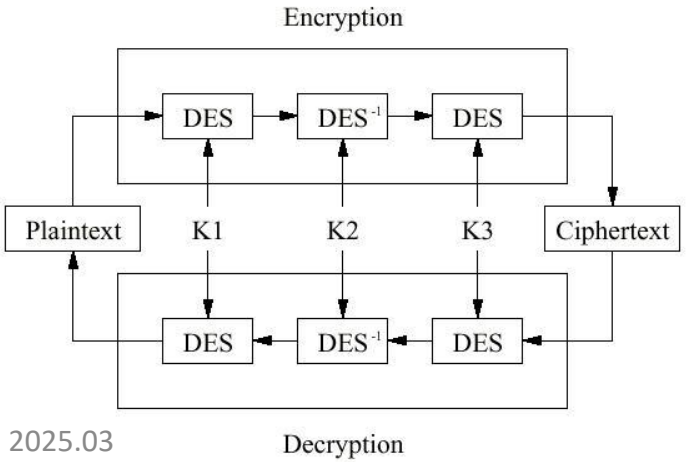
Criptografia Simétrica – Cifras por Blocos



- Cifras por Blocos (Algoritmos populares)
  - DES (Data Encryption Standard)
    - Definido em 1977 e utilizado extensivamente durante décadas, nomeadamente pelo sector financeiro
    - Utiliza chaves de 64 bits, em que apenas 56 são úteis (dado que 8 são usados para paridade)
    - Tamanho de bloco: 64 bits Iterações: 16
    - Atualmente a sua utilização é francamente desaconselhada, dado ser vulnerável a ataques de força bruta (devido à reduzida dimensão das chaves), de criptoanálise diferencial/linear e de técnicas específicas (Improved Davies' Attack), sendo possível construir um equipamento para o quebrar por cerca de 5.000€

Criptografia Simétrica – Cifras por Blocos

- Cifras por Blocos (Algoritmos populares)
  - Triple DES
    - Cifra em cascata que permite utilizar o DES com chaves de 56, 112 ou 168 bits úteis, consoante c1, c2 e c3 sejam iguais ou diferentes entre si
    - Apesar de ser bastante mais seguro do que o DES, é consideravelmente mais lento do que as alternativas existentes atualmente



Criptografia Simétrica – Cifras por Blocos

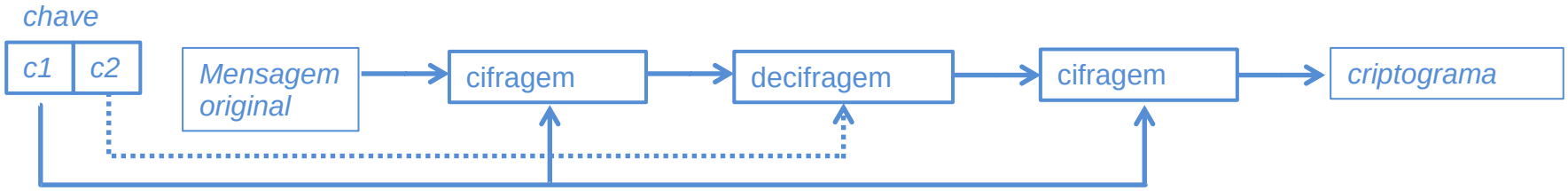
- Cifras por Blocos (Algoritmos populares)
  - AES (Advanced Encryption Standard)
    - Cifra que resultou de um concurso mundial promovido pelo NIST para substituir o DES e que culminou com a escolha do algoritmo Rijndael, de uma short list de 15 candidatos
    - Cada algoritmo candidato necessitava de:
      - Ser um algoritmo público e não sujeito a direitos de autor
      - Suportar chaves de 128, 192 e 256 bits
      - Utilizar blocos de 128 bits
      - Ter implementações eficientes em hardware e em software (C e Java) em três tipos de plataformas (smartcards, 32 bits e 64 bits)

Criptografia Simétrica – Cifras por Blocos

- Cifras por Blocos (Algoritmos populares)
  - AES (Advanced Encryption Standard) (animação)
    - É vulnerável a ataques de chaves relacionadas (quando se utiliza uma chave parecida/derivada da chave anterior), o que não é crítico desde que se utilizem sempre chaves aleatórias
    - Como a generalidade das cifras por blocos, a otimização da sua eficiência depende da utilização de substitution boxes (S-Box), o que aumenta a sua vulnerabilidade a side-channel attacks, em que se procura recolher informação (por exemplo da memória) que permita quebrar a chave
    - Iterações: 10, 12 ou 14 conforme tamanho da chave
    - Apesar de uma chave de 128 bits ser atualmente considerada segura, é recomendável a utilização de chaves de 256 bits

Criptografia Simétrica – Cifras por Blocos

- Cifras em Cascata
  - Permitem reduzir a eficácia de ataques de força bruta sobre algoritmos cujo tamanhos das chaves seja considerado insuficiente
  - Utilizam uma sequência de operações de cifragem e decifragem realizadas com chaves diferentes
  - Contudo, a segurança da cifra não aumenta na direta proporção do aumento no tamanho na chave, dado que este encadeamento de operações acarreta vulnerabilidades
  - São mais lentos do que algoritmos que suportem nativamente a utilização de chaves de tamanho superior

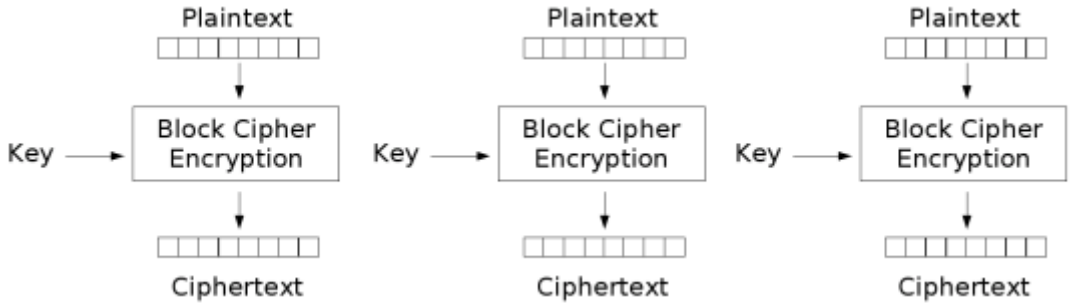


Criptografia Simétrica – Cifras por Blocos

Modo de Operação

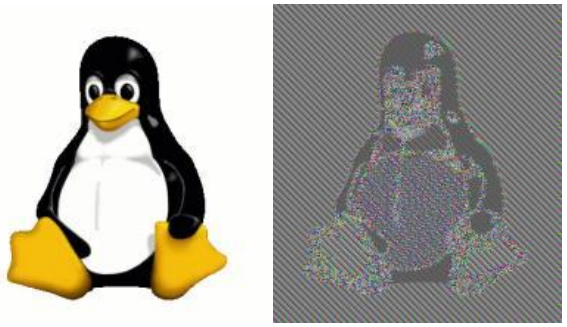
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo ECB (Electronic Code Book)
    - Um mesmo bloco é cifrado sempre do mesmo modo
    - Não esconde estereótipos da mensagem original (partes repetidas em posições fixas)



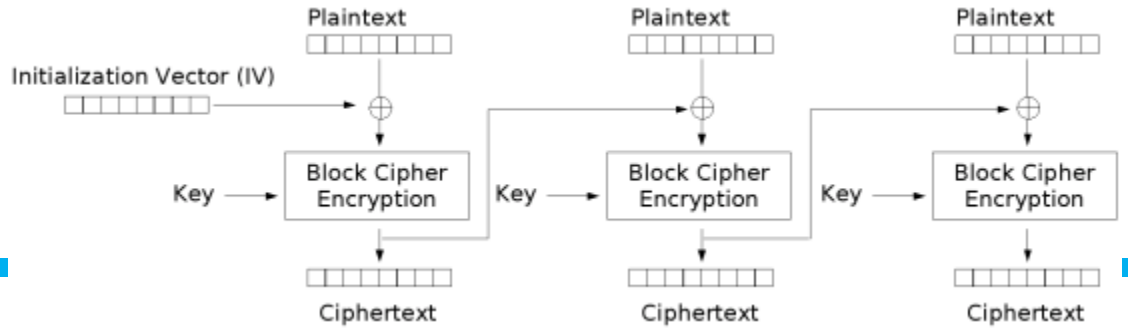
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo ECB (Electronic Code Book)
    - É vulnerável a ataques de repetição de blocos: Intruso força o envio pelo emissor de um bloco da sua escolha e reenvia-o repetidamente ao destinatário
    - Para ser considerado seguro não deve ser usado em mensagens superiores a 1 bloco
    - Não esconde padrões da mensagem original



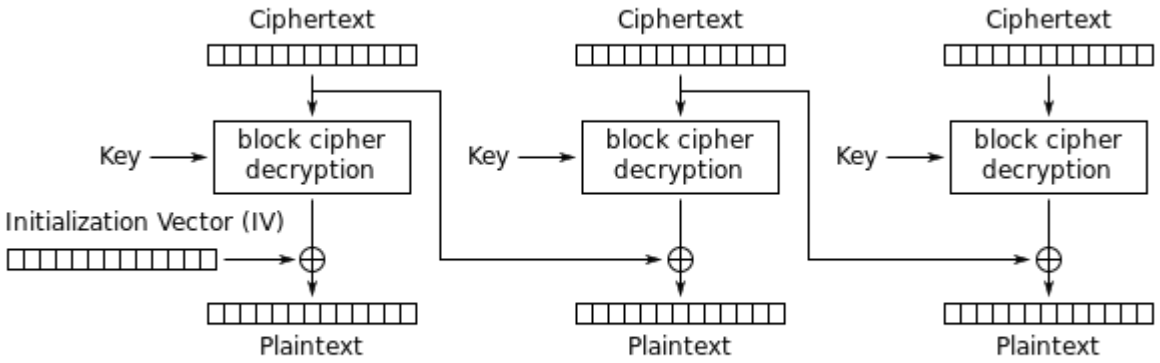
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo CBC (Cipher-Block Chaining)
    - Cifra-se o resultado do XOR entre cada bloco e o criptograma do bloco anterior
    - Para o primeiro bloco utiliza-se um vetor de inicialização (definido em conjunto com a chave) em substituição do criptograma anterior
    - É o modo mais utilizado, apesar de a sua natureza sequencial impedir o paralelismo (da cifragem) e de eventuais erros de cifra/ comunicação serem propagados e corromperem os blocos seguintes



Criptografia Simétrica – Modo de Operação

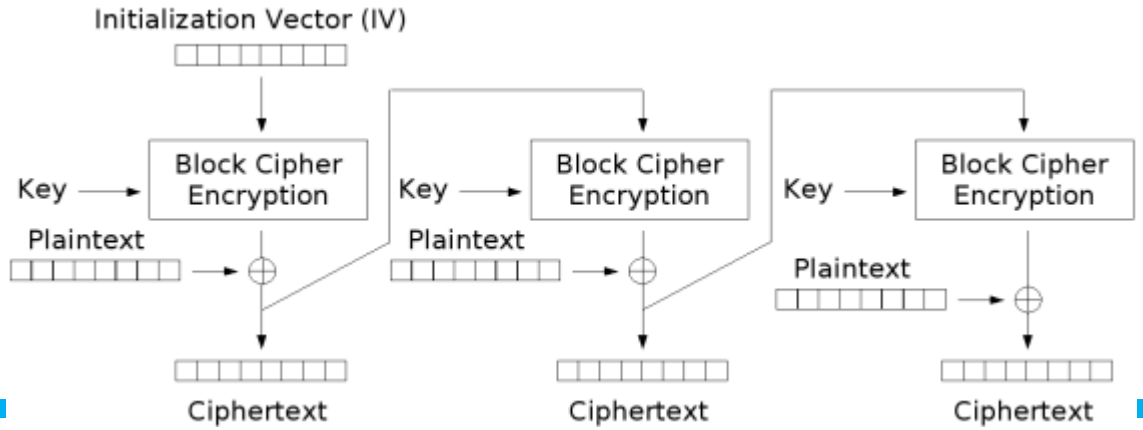
- Cifras por Blocos – Modos de Operação
  - Modo CBC (Cipher-Block Chaining - decryption)



Cipher Block Chaining (CBC) mode decryption

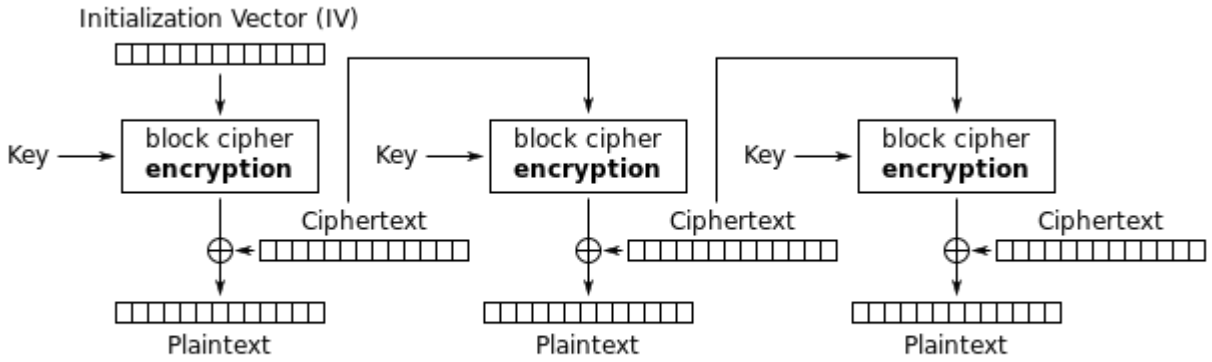
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo CFB (Cipher FeedBack)
    - Derivado do CBC, transforma a cifra de blocos numa cifra sequencial auto sincronizável (tem a vantagem de não necessitar da realização de padding)
    - Cada criptograma resulta do XOR entre o criptograma do bloco anterior e a chave calculada por um gerador de chaves, que por sua vez é alimentado pelo criptograma anterior



Criptografia Simétrica – Modo de Operação

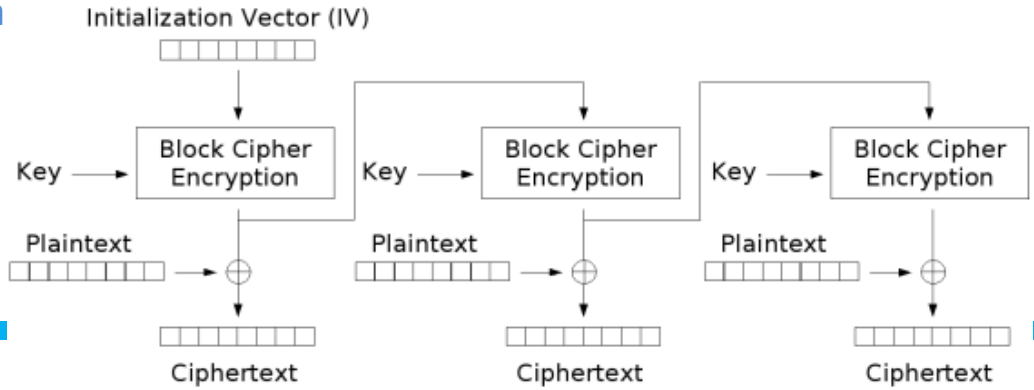
- Cifras por Blocos – Modos de Operação
  - Modo CFB (Cipher FeedBack - decryption)



Cipher Feedback (CFB) mode decryption

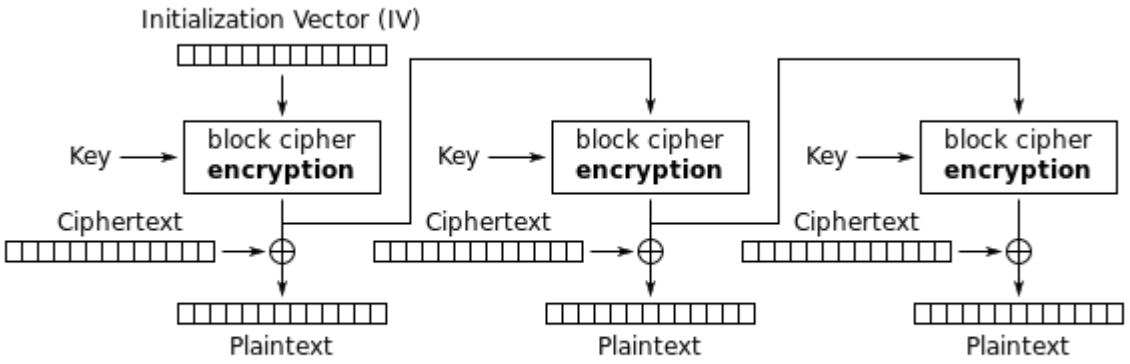
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo OFB (Output FeedBack)
    - À semelhança do CFB, também transforma a cifra de blocos numa cifra sequencial auto sincronizável
    - Contudo, neste caso o gerador de chaves é alimentado pelas chaves que gera (e não pelos criptogramas)
    - Dada a simetria do XOR, as operações de cifragem e decifragem implementam-se exatamente da mesma forma



Criptografia Simétrica – Modo de Operação

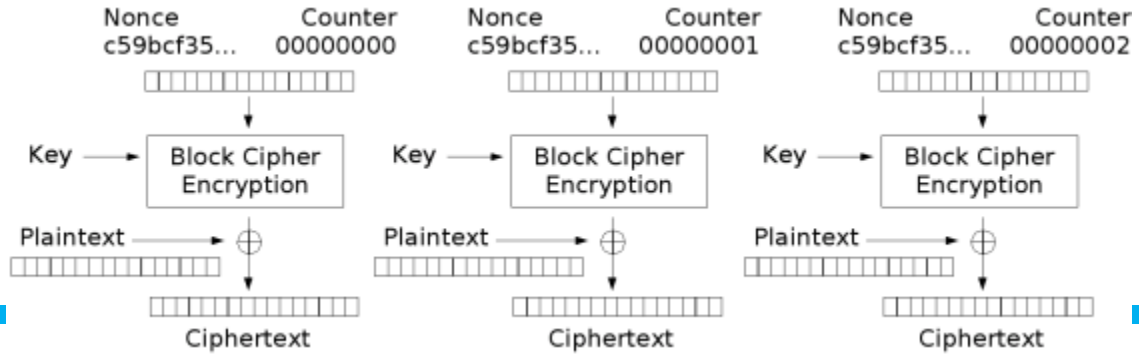
- Cifras por Blocos – Modos de Operação
  - Modo OFB (Output FeedBack - Decryption)



Output Feedback (OFB) mode decryption

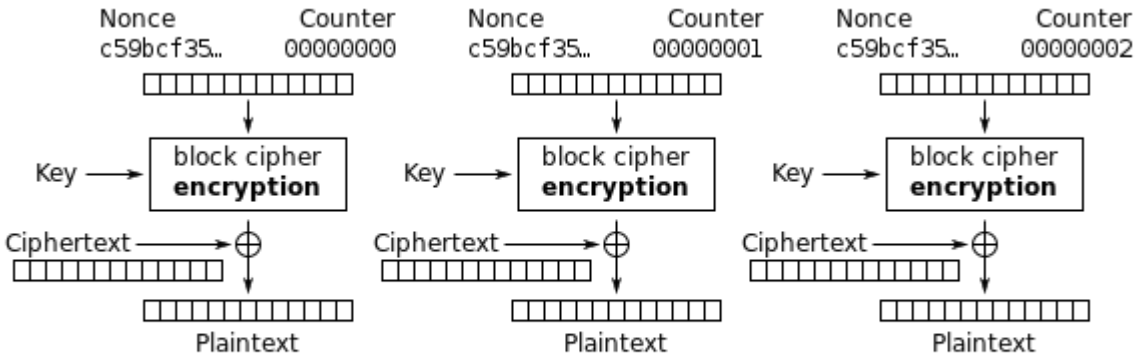
Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo CTR (Counter)
    - À semelhança do CFB, também transforma a cifra de blocos numa cifra sequencial auto sincronizável
    - Contudo, neste caso o gerador de chaves é alimentado pela composição entre um nonce (vetor de inicialização) e um contador (e não pelos criptogramas)
    - É mais seguro do que o CBC porque impede que um atacante injete ou retire blocos



Criptografia Simétrica – Modo de Operação

- Cifras por Blocos – Modos de Operação
  - Modo CTR (Counter - decryption)



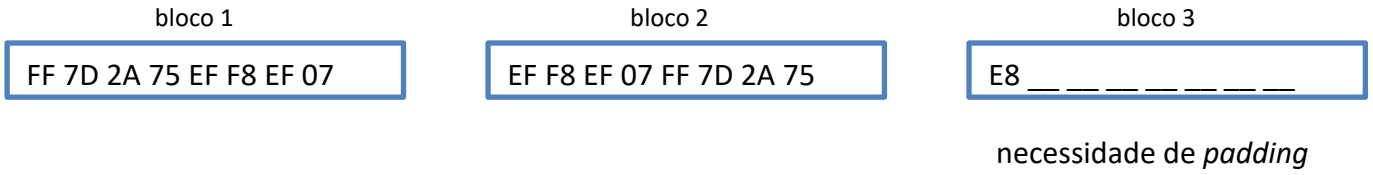
Counter (CTR) mode decryption

Criptografia Simétrica – Cifras por Blocos

Padding

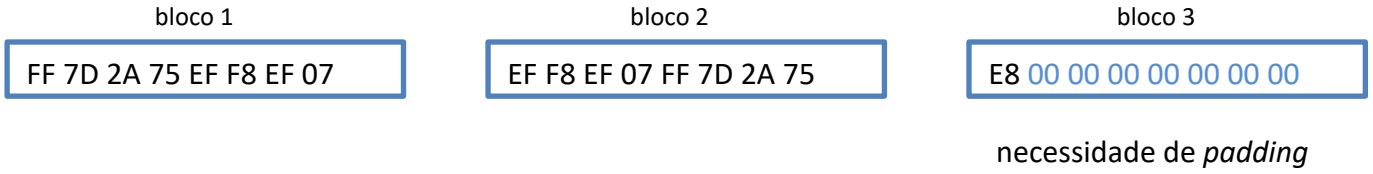
Criptografia Simétrica – Padding

- Esquemas de Padding
  - Necessidade
    - Dada a sua natureza, as cifras de blocos apenas permitem cifrar conjuntos de *n* bits
    - Assim, sempre que o texto original não for múltiplo de *n*, é necessário preencher os bits que restantes, recorrendo a um determinado esquema de padding
    - Contudo, esse processo deve ser efetuado de uma forma que permita a sua reversibilidade, no sentido de assegurar a recuperação exata e sem adulteração da mensagem original



Criptografia Simétrica – Padding

- Esquemas de Padding - Algoritmos mais populares
  - Zero Byte Padding
    - É o processo mais simples, consistindo apenas no acréscimo de bytes 00 até completar o tamanho do bloco
    - A sua utilização é desaconselhada dado que:
    - Poderá não ser completamente reversível (caso o último byte da mensagem original seja também um byte 0)
    - Poderá contribuir para a quebra da chave, caso o padding seja efetuado para um elevado número de bytes



Criptografia Simétrica – Padding

- Esquemas de Padding - Algoritmos mais populares
  - PKCS#7
    - Definido no RFC 5652
    - Consiste na adição de bytes cujo valor corresponde ao número de bytes de padding acrescentados
    - Exemplo:

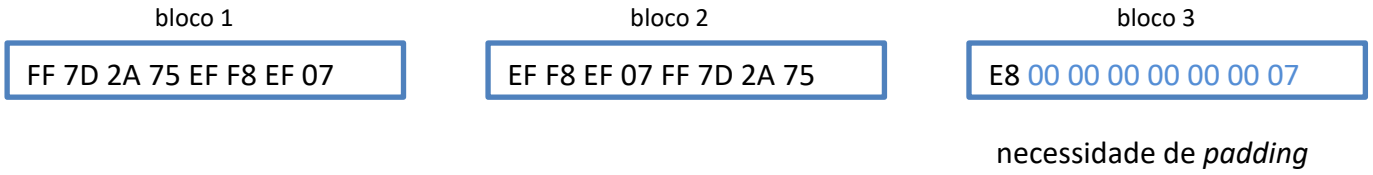
01
02 02
03 03 03
04 04 04 04
05 05 05 05 05
…

bloco 1	bloco 2	bloco 3
FF 7D 2A 75 EF F8 EF 07	EF F8 EF 07 FF 7D 2A 75	E8 07 07 07 07 07 07 07

necessidade de *padding*

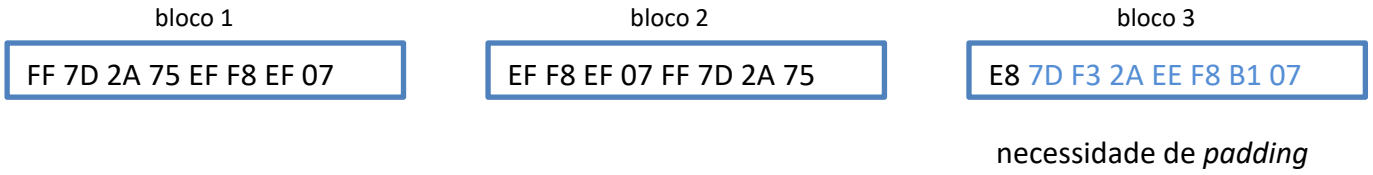
Criptografia Simétrica – Padding

- Esquemas de Padding - Algoritmos mais populares
  - ASNI X9.23
    - Consiste na adição de uma sequência de bytes 00, terminada com um byte que identifica o comprimento da sequência de padding
    - Exemplo (para um bloco de 8 bytes):



Criptografia Simétrica – Padding

- Esquemas de Padding - Algoritmos mais populares
  - ISO 10126-2
    - Consiste na adição de uma sequência de padding aleatória, terminada com um byte que identifica o comprimento da sequência de padding
    - Exemplo (para um bloco de 8 bytes):



Criptografia Simétrica

Bugs & Vulns

Questões?

Criptografia Simétrica – Prática

- Teórico-Prática
  - Exercicio de Criptografia Simétrica em Java
    - Java 8 (ou superior // last update)
    - Eclipse ou
    - Netbeans

Criptografia Simétrica – Prática

- Teórico-Prática
  - Exercício de Criptografia Simétrica em Java – Criar classe que permita:
    - Gerar chaves
    - Cifrar
    - Decifrar
    - Especificar:
      - algoritmo
      - modo
      - Padding
    - Opcional:
      - Gravar para ficheiro
      - Ler de ficheiro