Introdução às Cifras por Blocos

Definição (Cifras por Blocos)

Uma n-bit cifra por blocos *é uma função* $E : V_n \times \mathcal{K} \to V_n$*, tal que para cada k-bit* $K \in \mathcal{K}$*,* $E(P, K)$ *é uma função invertível (a* função de encriptação *para* K*) de* V_n *para* V_n*, denotada por* $E_K(P)$*. A função inversa é a* função de desencriptação*, denotada* $D_K(C)$*.*

A expressão $C = E_K(P)$ *denota o facto de que o texto cifrado* C *resulta da encriptação do texto claro ("plaintext")* P*, usando-se para tal a chave* K*.*

- n é designado o *comprimento do bloco*.
- A utilização de blocos de igual comprimento tanto para o texto claro como para o texto cifrado evita a expansão da informação.

Cifra Aleatória

Sempre que o comprimento da mensagem a cifrar ultrapassa o comprimento do blocos é necessário dividir a mensagem em blocos, as formas de o fazer será discutida à frente.

Definição (Cifra Aleatória)

Uma (verdadeira) cifra aleatória *é uma cifra por blocos que implementa todas as* $2^n!$ *bijecções de* 2^n *elementos. Cada uma das* $2^n!$ *chaves, especifíca uma dessas bijecções.*

Uma cifra deste tipo requereria $\log_2(2^n!) \approx (n - 1{,}44)2^n$ bits, ou aproximadamente 2^n-vezes o número de bits de um bloco da mensagem. O valor excessivo que isso representa torna este tipo de cifra impraticável.

Cifra Aleatorizada

Definição (Cifra Aleatorizada)

Uma cifra aleatorizada *é uma função* E *de um espaço de textos claros* V_n*, para um espaço de textos cifrados* V_m*,* $m > n$*, com o retirar de elementos de um espaço de números aleatórios* $\mathcal{R} = V_t$*.*
E *é definida por*

$$E : V_n \times \mathcal{K} \times \mathcal{R} \to V_m,$$

tal que, para cada chave $k \in \mathcal{K}$ *e* $R \in \mathcal{R}$*,* $E(P, K, R)$*, também escrita como,* $E_K^R(P)$*, aplica* $P \in V_n$ *a* $C \in V_m$*; e existe uma função inversa (função de desencriptação), de* $V_m \times \mathcal{K} \to V_n$*.*

Cifra Aleatorizada

Uma cifra por blocos (simples) é uma função determinística, cada par de texto claro P e chave K é transformado num único texto cifrado. Em contraste uma cifra aleatorizada associa o par (P, K) com um conjunto de $C_{(P,K)}$ de blocos cifrados elegíveis, sempre que P é cifrado, com uso da chave K, o resultado de um gerador aleatório R escolhe, de forma não determinística um dos blocos elegíveis.

De forma a garantir a invertibilidade, para cada chave fixa K, e para todo o texto claro P os sub-conjuntos $C_{(P,K)}$ têm de ser disjuntos.

Esta técnica implica expansão da informação.

Modos de Preenchimento

Uma cifra por blocos encripta os textos claros em blocos de comprimento fixo com n-bits (usualmente $n = 64$), para mensagens que excedam esse comprimento a mensagem é particionada em blocos de comprimento n-bits, sendo cada um dos blocos encriptado de forma separada.

Se o comprimento da mensagem não for um múltiplo de n é necessário preencher de alguma forma a mensagem de forma a que tenhamos um múltiplo de n.

Modos de Preenchimento

Método de Preenchimento 1

ENTRADA: x, texto claro; n, comprimento (em bits) do bloco.
SAÍDA: x_0, texto claro preenchido de forma a ter um comprimento múltiplo de n.

1. Concatenar a x o menor número de (possivelmente zero) 0-bits necessários para obter um texto cujo comprimento seja um múltiplo de n.

Método de Preenchimento 2

ENTRADA: x, texto claro; n, comprimento (em bits) do bloco.
SAÍDA: x_0, texto claro preenchido de forma a ter um comprimento múltiplo de n.

1. Concatenar a x um único 1-bit.
2. Concatenar de seguida o menor número de (possivelmente zero) 0-bits necessários para obter um texto cujo comprimento seja um múltiplo de n.

Prós e Contras dos Métodos de Preenchimento

- *O método de preenchimento 1 é ambíguo* - os eventuais 0-bits no fim do texto original não se conseguem distinguir daquelas que foram acrescentados no processo de preenchimento. Um tal método é aceitável se o comprimento do texto claro (antes do preenchimento) é sabido, por outros meios, pelo destinatário da mensagem.

- *O método 2 não é ambíguo*. Quando o comprimento do texto original é já um múltiplo do comprimento do bloco, *resulta do método a criação de um bloco extra*.

Modos de Operação

Os métodos mais usuais de particionar uma mensagem em blocos são:

ECB "**E**lectronic **C**ode**B**ook".

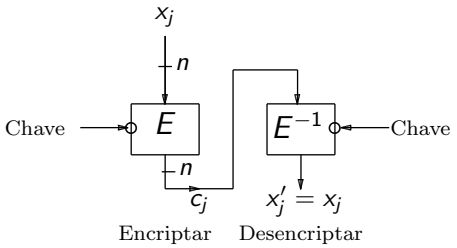
CBC "**C**ipher-**B**lock **C**haining".

CFB "**C**ipher **F**eed**B**ack".

Existem outros modos: Output FeedBack (**OBF**); Counter Mode (**CTR**); Offset-Codebook Mode (**OCM**).

Modo de Operação ECB

Electronic **C**ode**b**ook (ECB) — uma mensagem é particionada em blocos de comprimento n-bit e estes são encriptados separadamente.



Algoritmo ECB

ENTRADA: chave de comprimento k (bits), blocos de comprimento n (em bits) de texto claro, $x_1, \ldots x_t$.
SAÍDA: produz blocos de texto cifrados $c_1, \ldots, c_t$

1. Cifrar: para $1 \leq j \leq t$, $c_j \leftarrow E_K(x_j)$.
2. Decifrar: para $1 \leq j \leq t$, $x_j \leftarrow E_K^{-1}(c_j)$.

Propriedades do Modo de Operação ECB

Propriedades do modo de operação ECB:

1. Blocos de texto claro idênticos: sob a mesma chave resultam em blocos cifrados idênticos.
2. Dependências entre blocos: os blocos são cifrados de forma independente entre si. A re-ordenação dos blocos de texto cifrado resulta no re-ordenamento dos blocos de texto claro.
3. Propagação de Erros: um ou mais erros em bits num único bloco de texto cifrado afecta somente esse bloco. Para uma cifra típica E, o desencriptar de um tal bloco é então aleatório (com cerca de 50% de recuperação de texto claro).
4. Perdas de informação: a recuperação de bits "perdidos" nas fronteiras dos blocos não é possível.

Propriedades do Modo de Operação ECB

Nota (Utilização do modo ECB)

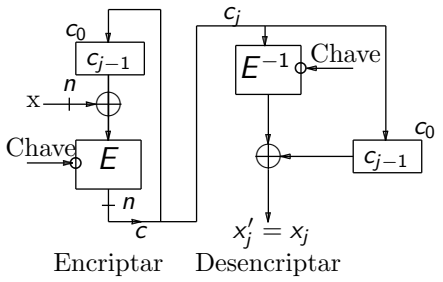
Dado que os blocos de texto cifrado são independentes uns dos outros a substituição maliciosa de blocos no modo ECB (por exemplo a inserção de um bloco muito frequente) não afecta a desencriptação dos blocos adjacentes. Mais, os blocos cifrados não escondem os padrões, isto é blocos cifrados idênticos implicam blocos de texto claro idênticos. Por esta razão o modo ECB não é recomendável para mensagens de comprimento maior do que um bloco, ou nos casos em que a chave é usada mais do que uma vez.

Nota (re-sincronização vs. erros nas fronteiras)

Por re-sincronização entende-se a recuperação por erros (sem perda de informação) nos blocos. Por erros nas fronteiras entende-se a "perda" de bits nas fronteiras dos blocos.

Modo de Operação CBC

Cipher-**b**lock **C**haining — utiliza um vector de inicialização de n-bits.



Algoritmo CBC

ENTRADA: K, chave de comprimento k (bits), n_0 bloco inicial de comprimento n-bits, blocos de comprimento n (em bits) de texto claro, $x_1, \ldots x_t$.
SAÍDA: produz blocos de texto cifrados $c_1, \ldots, c_t$.

1. Cifrar: $c_0 \leftarrow n_0$. Para $1 \leq j \leq t$, $c_j \leftarrow E_K(c_{j-1} \oplus x_j)$.
2. Decifrar: $c_0 \leftarrow n_0$. Para $1 \leq j \leq t$, $x_j \leftarrow c_{j-1} \oplus E_K^{-1}(c_j)$.

Propriedades do Modo de Operação CBC

Propriedades do Modo de Operação CBC:

1. Blocos de texto claro idênticos: sob a mesma chave e bloco inicial resultam em blocos cifrados idênticos. Mudando o bloco inicial, a chave, ou um primeiro bloco de texto claro (por exemplo, com um entrada aleatória) resulta num texto cifrado diferente.
2. Dependências entre blocos: a dependência entre blocos faz com que o texto cifrado c_j dependa de x_j e de todos os blocos de texto claro precedentes. O re-ordenar dos blocos de texto cifrado afecta a correcta decifração do texto global.
3. Propagação de erros: um erro num único bit no texto cifrado c_j afecta o decifrar dos blocos c_j e c_{j-1}, isto dado que x_j depende de c_j e de c_{j-1}. Nessas condições o bloco x_j, recuperado de c_j, é tipicamente, aleatório (50% errados), e o bloco x_{j+1} tem um bit errado precisamente aonde o bloco c_j tinha. O adversário pode então planear uma alteração no bloco x_{j+1}, alterando para tal o bloco c_j.
4. Recuperação de erros: um erro (incluindo a perda de um ou mais blocos) num bloco c_j afecta somente o bloco que se lhe segue de imediato, o bloco c_{j+2} não é afectado pelo erro ocorrido em c_j.

Propriedades do Modo de Operação CBC

Nota (Propagação de Erros na Encriptação)

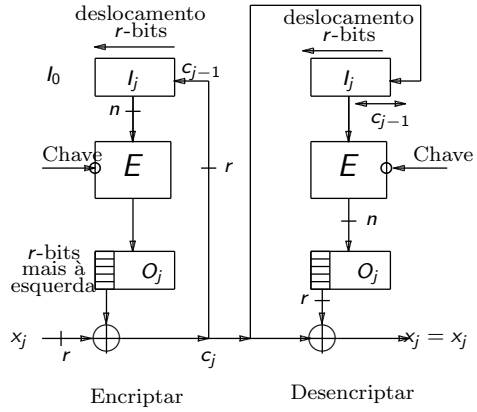
Embora o modo CBC consiga recuperar de erros nos blocos cifrados, modificações no bloco de texto claro x_j durante a encriptação alteram os blocos cifrados subsequentes. Isto tem efeitos na usabilidade dos modos com encadeamento para aplicações que requeiram acessos aleatórios de leitura/escrita à informação encriptada. O modo ECB é uma alternativa nesses casos.

Nota (Integridade do Vector de Inicialização em CBC)

Enquanto que o vector de inicialização no modo CBC não necessita de permanecer secreto, a sua integridade tem de ser protegida, isto dado que modificações maliciosas ao mesmo permitem ao adversário fazer modificações (em bits) previsíveis ao primeiro bloco de texto claro recuperado. Usar um vector de inicialização secreto é uma forma de impedir isso, no entanto se a integridade da mensagem é um requerimento é necessário usar um outro tipo de mecanismo.

Modo de Operação CFB

Cipher **f**eed**b**ack (CFB) — r-bit caracteres/r-bit re-alimentação. Enquanto o modo CBC processa o texto claro n bits de cada vez (usando uma cifra de blocos de comprimento n), algumas aplicações podem requerer que um bloco de r-bits seja encriptado e transmitido sem demoras, para um dado $r < n$ (usualmente $r = 1$ ou $r = 8$).



Modo de Operação CFB

Algoritmo CFB

ENTRADA: K, chave de comprimento k (bits), I_0 bloco inicial de comprimento n-bits, blocos de comprimento r-bits de texto claro, $x_1, \ldots x_t$, $1 \leq r \leq n$.
SAÍDA: produz blocos, de comprimento r-bits, de texto cifrados $c_1, \ldots, c_t$.

1. Cifrar: $I_1 \leftarrow I_0$ (I_1 é o valor no registo de deslocamento, para $1 \leq j \leq t$).
   1. $O_j \leftarrow E_k(I_j)$ (cálculo do resultado da cifra por blocos).
   2. $o_j \leftarrow$ os r-bits mais à esquerda de O_j
   3. $c_j \leftarrow x_j \oplus o_j$ (transmite o bloco cifrado, de comprimento r-bits, c_j).
   4. $I_{j+1} \leftarrow 2^r \cdot I_j + c_j \mod 2^n$ (desloca c_j para o lado esquerdo do registo de deslocamento).
2. Decifrar: $I_1 \leftarrow I_0$. Para $1 \leq j \leq t$, $x_j \leftarrow c_j \oplus o_j$, aonde o_j, O_j, e I_j são calculados da forma já descrita.

Propriedades do Modo de Operação CFB

Propriedades do modo de operação CFB.

1. Blocos de texto claro idênticos: assim como para o modo de operação CBC a mudança do bloco inicial resulta num bloco cifrado diferente. O bloco inicial não necessita de ser secreto.
2. Dependências entre blocos: similar ao modo de operação CBC, o bloco c_j depende dos blocos x_j e x_{j-1}. Consequentemente o re-ordenar dos blocos cifrados afecta a decifração. Para uma correcta decifração é necessário que os $\lceil n/r \rceil$-blocos precedentes estejam correctos (de forma a que o registo de deslocamento contenha um valor correcto).

Propriedades do Modo de Operação CFB

Propriedades do modo de operação CFB (continuação).

3. Propagação de erros: um ou mais bits num único r-bit bloco cifrado c_j afecta a desencriptação desse e dos próximos $\lceil n/r \rceil$ blocos cifrados, ou seja até que n bits de texto cifrado sejam processados, após o que o bloco com erros c_j foi deslocado para fora do registo de deslocamento. O texto claro recuperado x_j vai deferir do bloco original x_j precisamente na posição (em bits) na qual c_j contém o erro; os outros blocos de texto claro incorrectamente recuperados são tipicamente vectores aleatórios, i.e. têm 50% de bits em erro. Consequentemente um adversário podem causar modificações previsíveis num dado bit de x_j, por alteração do bit correspondente em c_j.

Propriedades do Modo de Operação CFB

Propriedades do modo de operação CFB (continuação).

4. Recuperação de erros: o modo CFB é auto-sincronizável, de forma similar ao CBC, mas requer $\lceil n/r \rceil$ de blocos cifrados para recuperar.
5. Débito: para $r < n$, o débito decresce por um factor de n/r (vs. CBC) dado que cada execução de E só dá origem a r bits de texto cifrado.

Nota (CFB e a Função de Encriptação)

Dado que a função de encriptação E é usada, no modo CFB, tanto para a encriptação como para a desencriptação, este modo não pode ser usado em conjunção com cifras de chave pública. Nesses casos deve-se usar o modo CBC.

Encriptação Múltipla

Se uma cifra por blocos é susceptível a um ataque por procura exaustiva da chave (devido a um comprimento da chave inadequado), então a encriptação do mesmo bloco mais do que uma vez pode aumentar a segurança.

As técnicas para a encriptação múltipla podem ser usadas em conjunção com os modos de operação já estudados, o E passa a denotar a encriptação múltipla em vez de simples.

Cifras em Cascata

Definição (Cifras em Cascata)

Uma cifra em cascata *é a concatenação de $L \geq 2$ cifras por blocos (designados por estágios) cada uma com uma chave independente. O texto claro é a entrada para o primeiro estágio, sendo a saída deste estágio a entrada do seguinte. A saída do estágio L é a saída da cifra em cascata.*

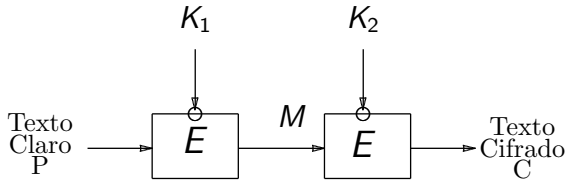
No caso mais simples, todos os estágios numa cifra em cascata têm chaves de comprimento k, e blocos de comprimento n. As cifras de cada estágio podem ser diferentes (cifra em cascata genérica), ou serem todas a mesma (cascata de cifras idênticas).

Encriptação Múltipla

Definição (Encriptação Múltipla)

A encriptação múltipla *é similar à cascata de L cifras idênticas, mas os estágios podem não ser independentes, e para um dado estágio podemos ter a função de encriptação E ou a sua correspondente inversa $D = E^{-1}$.*

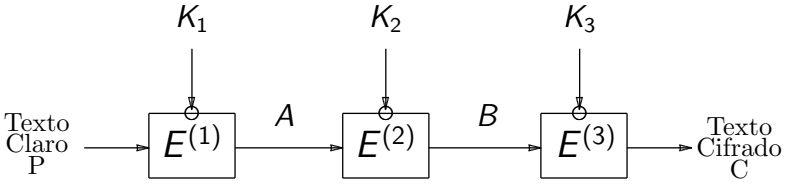
Dois casos importantes de múltipla encriptação são a dupla e tripla encriptação.



Definição (Dupla Encriptação)

A dupla encriptação *é definida por $E(x) = E_{K_2}(E_{K_1}(x))$, aonde E_k denota uma cifra por blocos E com chave K.*

Encriptação Múltipla



Definição (Tripla Encriptação)

A tripla encriptação *é definida por $E(x) = E^{(3)}_{K_3}(E^{(2)}_{K_2}(E^{(1)}_{K_1}(x)))$, onde $E^{(j)}_k$ denota ou E_k, ou $D_K = E^{-1}_k$. O caso $E(x) = E_{K_3}(D_{K_2}(E_{K_1}(x)))$, é usualmente designado por E-D-E tripla encriptação. O sub-caso $K_1 = K_3$ é usualmente designado por tripla encriptação de duas chaves.*

Encriptação Múltipla

Na dupla encriptação é usual usar dois estágios independentes K_1 e K_2.

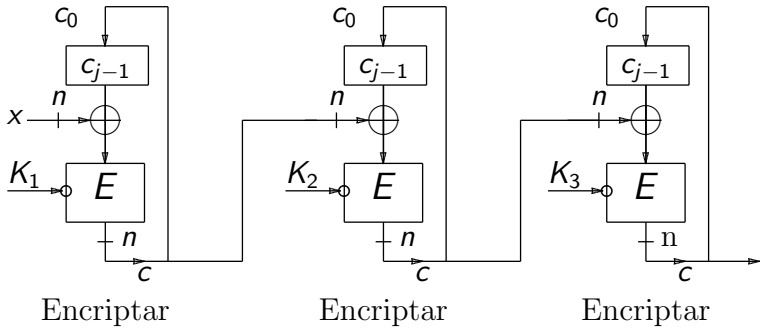
Na tripla encriptação, de forma a poupar recursos no que se refere à gestão de chaves, é usual usar chaves dependentes dos estágios.

A *E-D-E* tripla encriptação com $K_1 = K_2 = K_3$ é equivalente a uma encriptação simples.

Modos de Operação em Encriptação Múltipla

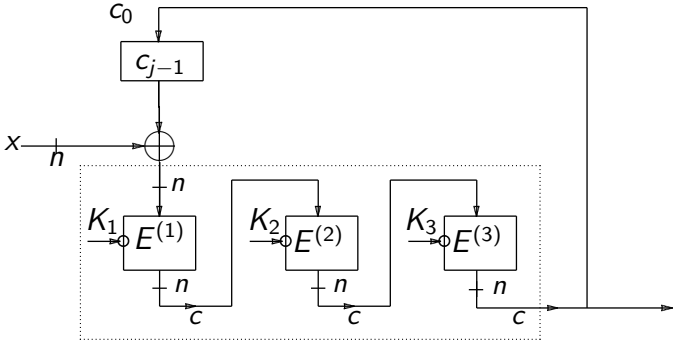
Em contraste ao modo de operação das cifras simples, os modos múltiplos são variantes de encriptações múltiplas construídas por concatenação de modos simples seleccionados.
Por exemplo, a combinação de três CBCs em modo de operação simples é designado por *CBC-triplo-interno*.

CBC-triplo-interno



Modos de Operação em Encriptação Múltipla

Uma alternativa é o modo designado por *CBC-triplo-externo*, em que temos a composição de uma encriptação tripla com um modo de operação simples, ou seja uma aplicação (externa) do modo de operação CBC, após a aplicação sequencial de três ECB.



Modos de Operação em Encriptação Múltipla

Com "hardware" específico (replicado), os modos múltiplos tais como o CBC-triplo-interno podem ser sequenciados ("pipelined"), permitindo deste modo uma eficiência próxima da encriptação simples, sendo por isso mais vantajoso que o CBC-triplo-externo.

Nota (Segurança do modo CBC-triplo-interno)

Muitos dos modos múltiplos de operação são mais fracos que o correspondente modo ECB múltiplo (isto é, encriptação múltipla a funcionar como uma só cifra para o modo de operação simples externo). Em alguns casos (por exemplo, ECB-CBC-CBC) não são significativamente mais fortes que uma encriptação simples.
Em particular, sob alguns tipos de ataques, o CBC-triplo-interno é significativamente mais fraco do que o CBC-triplo-externo.

Encriptação Múltipla

Embora pareça contra-intuitivo, é possível construir exemplos aonde uma cascata de cifras reduz a segurança. No entanto, em geral tem-se que:

Facto (Segurança de Cifras em Cascata)

Uma cascata de n (com chaves independentes) cifras é pelo menos tão segura como a primeira cifra componente. Uma cascata de cifras de permutações (por exemplo cifras aditivas) é tão segura como a componente mais segura.

Composição de Cifras

Uma forma de tentar aumentar a dificuldade de cripto-análise de uma cifra é dada pela composição de cifras.

A composição de involuções não é necessariamente uma involução. No entanto as involuções podem ser facilmente compostas de forma a se obter uma função de certa forma mais complicada e que é fácil de inverter.
Por exemplo, se $E_{k_1}, E_{k_2}, \ldots, E_{k_t}$ são involuções, então a inversa de $E_k = E_{k_1}, E_{k_2}, \ldots, E_{k_t}$ é $E_k^{-1} = E_{k_t}, E_{k_{t-1}}, \ldots, E_{k_1}$, isto é a composição das involuções pela ordem inversa.

Cifras Produto

As cifras simples de substituição e de transposição não são muito seguras. No entanto a combinação delas pode criar cifras bastante mais seguras do que as cifras de partida.

Cifra Produto

Sejam $\mathcal{M} = \mathcal{C} = \mathcal{K}$ o conjunto de todas as sequências binárias de comprimento 6. O número de elementos de $\mathcal{M}$ é $2^6 = 64$. Seja $m = (m_1 m_2 \ldots m_6)$ e sejam:

$$\begin{aligned} E_k^{(1)}(m) &= m \oplus k, \text{aonde } k \in \mathcal{K}, \\ E^{(2)}(m) &= (m_4 m_5 m_6 m_1 m_2 m_3). \end{aligned}$$

A operação denotada $\oplus$ é o *ou-exclusivo (XOR)*. $E_k^{(1)}$ é uma cifra de substituição poli-alfabética, $E^{(2)}$ é uma cifra de transposição (sem chave). A cifra produto é dada por $E_k^{(1)} E^{(2)}$.

Na terminologia inglesa designa-se este tipo de cifras um "round".

Confusão e Difusão

Definição (Confusão)

Uma cifra é dita adicionar confusão *sempre que aumentar a complexidade da relação entre a chave e o texto cifrado.* Uma cifra de substituição adiciona confusão a uma cifra produto.

Definição (Difusão)

A difusão *refere-se ao espalhar dos "bits" numa mensagem de forma que qualquer redundância no texto claro seja espalhada ao longo do texto cifrado.* Uma cifra de transposição adiciona difusão a uma cifra produto.

Temos então que uma cifra produto composta de uma substituição e de uma transposição adiciona confusão e difusão ao processo de encriptação.

Exercício Prático 5

Implemente a seguinte cifra produto.

Cifra Produto

Sejam $\mathcal{M} = \mathcal{C} = \mathcal{K}$ o conjunto de todas as sequências binárias de elementos com 16 bits de comprimento (dois "bytes").

$$\begin{aligned} E_k^{(1)}(m) &= m \oplus k, \text{aonde } k \in \mathcal{K}, \\ E^{(2)}(m) &= (m_{13} m_{14} m_{15} m_{16} m_9 m_{10} m_{11} m_{12} m_5 m_6 m_7 m_8 m_1 m_2 m_3 m_4). \end{aligned}$$

A cifra produto é dada por $E_k^{(1)}(E^{(2)}(m))$.

- Preenchimento não âmbiguo.
- Modo de operação ECB.
- Introdução de uma chave pelo utilizador.
- Interface Entrada/Saída: ficheiros e linha de comando.
- Implementação (cifrar/decifrar) em C (ou C++).