CIFRAS DE SUBSTITUIÇÃO

Definição

É uma forma de criptografia do qual as unidades de texto plano são substituídas por um texto cifrado de acordo com um sistema fixo (alfabeto). As unidades de texto podem ser pares, trios, quadras (...) de letras. Sua forma de decriptação é fazendo a substituição inversa.

O alfabeto do texto plano não é necessariamente coincidente ao do texto cifrado. Ex:

Alfabeto texto plano: ABCDEFGHI (...)

Alfabeto texto cifrado: 123456789 (...)

Substituição e transposição

SUBSTITUIÇÃO - POSIÇÃO PRESERVADA, ALFABETO ALTERADO

TRANSPOSIÇÃO - POSIÇÃO ALTERADA, ALFABETO PRESERVADO

EX.

Texto plano = Elefante

Substituição simples (deslocamento 1) = Fmfgborf

Transposição (espelho) = etnafelE

Substituição monoalfabética

Cada elemento do texto plano é mapeado para um elemento dum dado alfabeto (que não necessariamente é coincidente ao do texto plano). Ex:

Alfabeto do texto plano: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabeto do texto cifrado: 1234EFGHIJKLMNOPQRSTUVWXYZ

Então as letras são deslocadas conforme uma razão n pelo alfabeto.

Um exemplo famoso de uso é a cifra de César.

Substituição polialfabética

Difere da monoalfabética por utilizar uma taxa de deslocamento diferente para pelo menos um dos caracteres.

Alfabeto do texto plano/cifrado: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Texto plano: Elefante

Cifra: Ganeshga

Texto cifrado: Klrjsuze

Um exemplo famoso é a cifra de Vigenere.

Substituição homófona

Cada letra do alfabeto do texto plano é correspondida pra mais do que um símbolo. É utilizado para dificultar uma análise estatística baseada na frequência.

Alfabeto do texto plano:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Alfabeto 1 do texto cifrado:	1234EFGHIJKLMNOPQRSTUVWXYZ
Alfabeto 2 do texto cifrado:	@#$ABCDEFGHIJKLMNOPQRSTUV
Alfabeto 3 do texto cifrado:	ZWYKLMNSPQ234FDJV=-915678CX

Texto cifrado: ‘Cifra curta’ -> 3JGS1 $VSU@

Substituição poligráfica

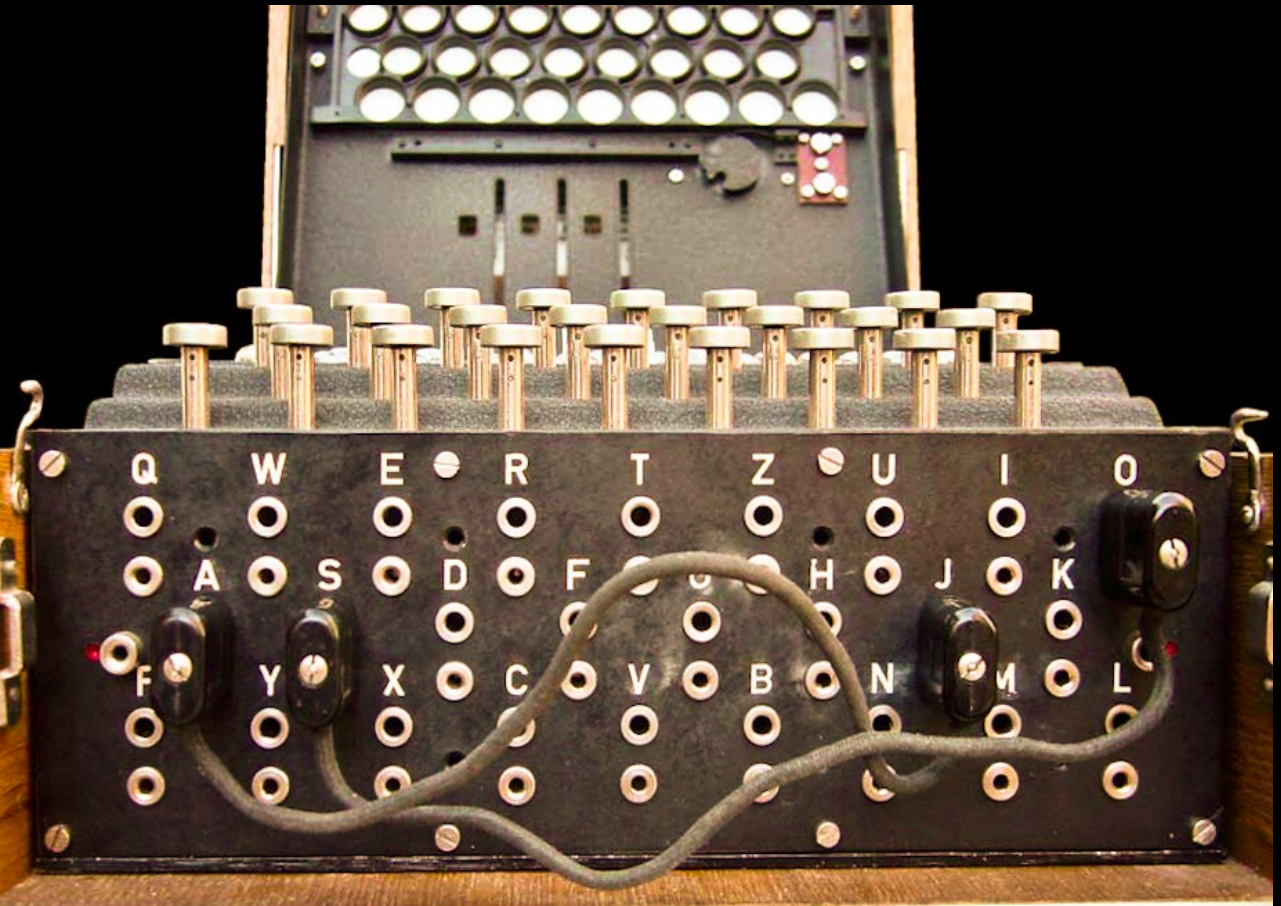
A substituição se dá mapeando um caractere para um grupo de símbolos.

Alfabeto do texto plano: A; B; C; E[...]

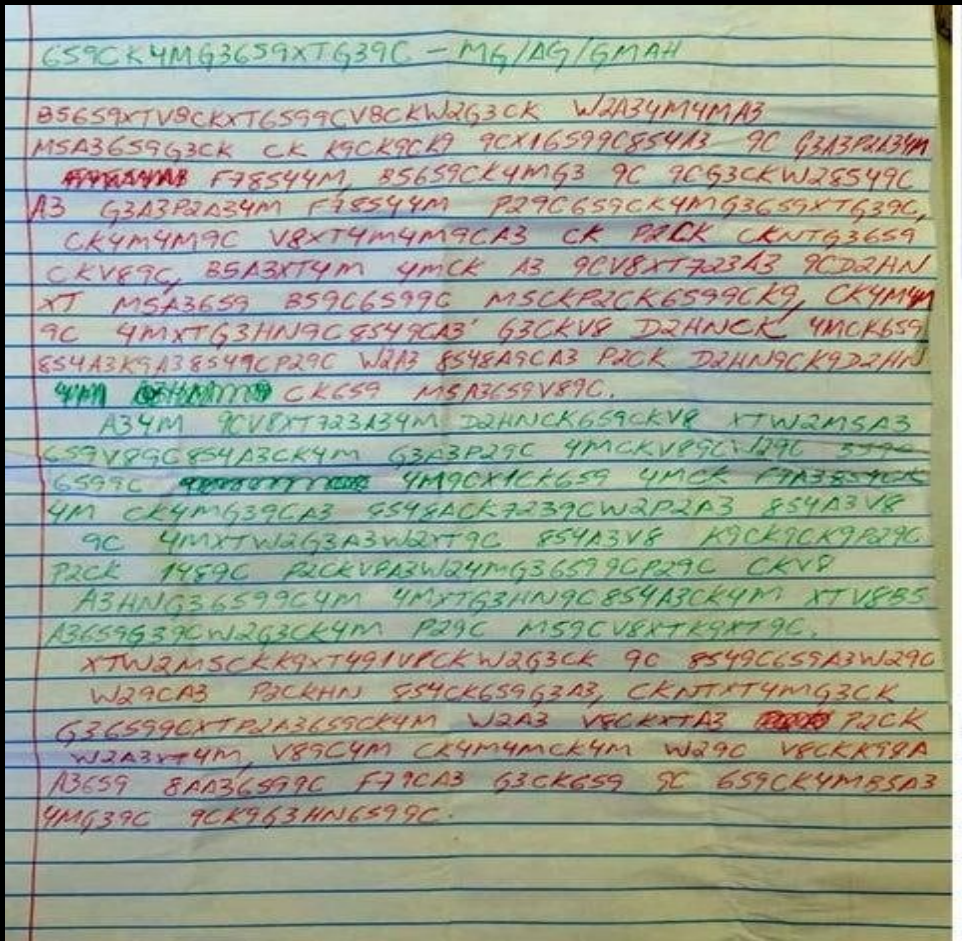
Alfabeto do texto cifrado: &A, 789; CVD; ZDFG[...]

Um exemplo famoso é a cifra de Hill.

Cifras de substituição mecânica



CARTA DO PCC



4M9CK9F7CK XT6594M P29C 659HN9C (A) CK4MB5CK659A3 D2HNCK CK4MG39C CKW2854A3W2G3659CK G3A3P2A34M 854A3V8 4M9CHNP2CK 9CB5CK4919C659 P2A3 K9HN7239C659. P2A3 B5CKP2XTP2A3 D2HNCK M5A3XT M5CKXTG3A3 B56599C K9CKF79CW2G39C659 9C 8549CV8XTW28A9CP29C P2A3 M56599CW2723A3, CK4M4MCK D2HNCK V8A36599C W29C V8CK4MV89C D2HNCKX16599CP29C P2CK F7A3854CKXT4M G39C W29C V89CA3. G3HNP2A3 A34M CKW2P2CK659CK854A3 D2HNCK CKK9CK F79CXT G39C V89CB5CK9CP2A3. CKK9CK V8A36599C W29C K99CHN4M V8CK4MV8A3 CK M5XT8549C 9C 4MCKV89CW29C G3A3P29C B5A3659 K99C B5A3659D2HNCK A3 G36599CV8B5A3 P2CKK9CK CK K99C P2CKW2G3659A3. P29C B56599C M59C491CK659 CKK9CK 8AA36599C D2HNCK D2HNXT 4MCK659, W2A3XT4M 1489C G3CKV8 A3 8549C659659A3, A34M A36599C659XTA3, G3HNP2A3 P2CKK9CK. A3HNG3659A3 4M9CK9F7CK. P2A3 M56599CW2723A3 1489CB5A3W2CKXT4M CK HNV8 B5A3HN854A3 V89CXT4M 854A3W2B5K9XT8549CP2A3, V89CXT4M P29C B56599C M59C491CK659 G39CV8X1CKV8 A36599C D2HNCK D2HNXT4MCK659. A3 D2HNCK G39C B5CK7239CW2P2A3 CK D2HNCK 9C 854XTP29CP2CK P2CKK9CK CK X1CKV8 V89CXTA3659 D2HNCK OP, B56599C P29C659 A3 X19CK99CA3 P2CKB5A3XT4M CK V89CXT4M P2XTM5XT854XTK9, V89CXT4M A34M XT6594M G39CA3 W2CK4M4M9C B5CK7239CP29C. A3 P2CK OP P29C B56599C M59C491CK659 A36599C D2HNCK F78544M M59CK99C D2HNCK CK 9C A36599C. CK W2A3XT4M.