Cifratura con codice a sostituzione

Dal testo in chiaro ogni lettera viene codificata con la sua posizione alfabetica (A = 1, B = 2,..., Z = 21), quindi si somma alla posizione una costante detta chiave (nell'esempio, il numero 3), trovando la lettera cifrata (p → 14; 14 + 3 = 17 → s).

La decifratura del testo avviene analizzando le singole lettere cifrate, trovandone la posizione e sottraendo 3 a quella posizione per individuare la lettera in chiaro (s → 17; 17 – 3 = 14 → p).

La cifratura con sostituzione cambia i simboli del testo in chiaro, ma ne mantiene l'ordine e la frequenza. Per esempio, la doppia 'oo' che compare nel testo cifrato corrisponde alla doppia 'll' del testo in chiaro.

«(...) So che ci sono persone che hanno fatto affari con terreni simili e con cifre più grosse, mi riferisco a shuvhrtahoorgnqdcfd e così per vie traverse ho cercato di sapere come si fa (...)».

Cifratura con codice a trasposizione

Il testo in chiaro viene disposto su righe di lunghezza pari alla chiave, nell'esempio AFRODITE. Per ogni carattere della chiave si trascrive la rispettiva posizione nell'alfabeto.

La cifratura avviene riportando il testo in chiaro per colonne, nell'ordine indicato dalle posizioni della chiave.

La cifratura con trasposizione mantiene gli stessi simboli del testo in chiaro, conserva la frequenza ma non ne conserva l'ordine.

A	F	R	O	D	I	T	E
1	*6*	*16*	*13*	*4*	*9*	*18*	*5*
s	***o***	***c***	***h***	***e***	***c***	***i***	***s***
o	***n***	***o***	***p***	***e***	***r***	***s***	***o***
n	***e***	***c***	***h***	***e***	***h***	***a***	***n***
n	***o***	***f***	***a***	***t***	***t***	***o***	***a***
f	***f***	***a***	***r***	***i***	***c***	***o***	***n***

«(...) sonnfceetisonanoneofcrhtchpharcocfaisaoo terreni simili e con cifre più grosse, mi riferisco a Perseo quello di Nazca e così per vie traverse ho cercato di sapere come si fa (...)».

Fin dai primi anni del secondo dopoguerra lo studioso *Claude Shannon* (*1916-2001*) indicò due criteri fondamentali per una cifratura ottimale: rendere la relazione tra chiave e testo cifrato molto complessa (**principio di confusione**) e rendere il rapporto tra testo in chiaro e testo cifrato molto complessa (**principio di diffusione**).

Per esempio, la cifratura con codice a sostituzione non rispetta il principio di diffusione: le sequenze delle doppie sono facilmente individuabili (nell'esempio la coppia «oo» rappresenta una «doppia» in italiano), così come le frequenze delle vocali.

I due principi si colgono meglio se espressi mediante il **criterio valanga** (*Avalanche Criterion*): affinché una cifratura sia efficiente è necessario che:

a) la modifica anche di un singolo simbolo della chiave, dovrebbe implicare l'alterazione di tutto il testo cifrato (*confusione*);
b) la modifica anche di un singolo simbolo del testo in chiaro dovrebbe implicare l'alterazione di tutto il testo cifrato (*diffusione*).

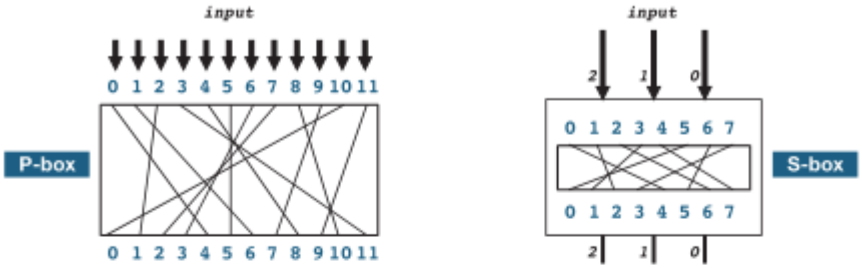
I moderni algoritmi di cifratura simmetrica utilizzano gli stessi principi di sostituzione e trasposizione, ma soddisfando il criterio *valanga*.

Gli algoritmi per generare i codici di cifratura simmetrica possono essere esemplificati con schemi denominati **P-box** (trasposizione) e **S-box** (sostituzione).

Crittografia con SPN

Sia data una P-box a 12 linee e una S-box a 3 bit, criptare i 12 bit 001110101001 con la chiave a 12 bit 011111000010 in due round.

Nel primo round si usi la chiave assegnata, nel secondo round si usi la chiave XOR 111111111111b.



La P-box traspone (sposta) i bit in base alle connessioni del diagramma: il primo bit a sinistra (posto 0) viene trasposto al posto 4; il secondo bit da sinistra (posto 1) viene trasposto al posto 6, ..., il dodicesimo bit da sinistra (posto 11) viene trasposto al posto 9.

La S-box permuta tre bit alla volta: se l'ingresso è la tripletta 110b (6 decimale), in base alle connessioni del diagramma, l'uscita vale 101b (5 decimale): la linea del posto 6 si congiunge al posto 5.

Ognuno dei due round consiste dei passi:

1. calcolo di: Testo XOR chiave;
2. applicazione della P-box;
3. applicazione della S-box.

Il Testo del primo round è il testo in chiaro.
Il Testo dei round successivi è il risultato del round precedente.
Al termine dell'ultimo round si ottiene il testo cifrato.

(In blu i dati; in neretto i risultati delle operazioni)

Round 1

Testo:	001 110 101 001 XOR
Chiave:	011 111 000 010
Testo XOR chiave:	**010 001 101 011**
Applicazione P-box:	**100 101 100 110**
Applicazione S-box:	**111 000 111 101**

Round 2

Testo:	111 000 111 101
Chiave:	011 111 000 010 XOR
	111 111 111 111
	100 000 111 101
Testo XOR chiave:	111 000 111 101 XOR
	100 000 111 101
	011 000 000 000
Applicazione P-box:	**010 000 100 000**
Applicazione S-box:	**110 100 111 100**

In definitiva:

testo in chiaro (*plaintext*):	001110101001
testo cifrato (*ciphertext*):	110100111100