AES

Advanced Encryption Standard (Rijndael): cifrario simmetrico a blocchi di 128 bit con chiavi da 128, 192 o 256 bit, in rispettivamente 10, 12 o 14 fasi identiche. Non ci sono attacchi noti migliori del brute force per versioni di AES con almeno 7 fasi, quindi tutti i bit della chiave sono di sicurezza.

AES 128

- ogni fase opera su un blocco di 128 bit, organizzato logicamente come matrice bidimensionale B di 16 byte (4×4), inizializzata con $m \oplus k$;
- la chiave iniziale è caricata *per colonne* in una matrice W di 4×4 byte, che poi viene ampliata aggiungendo altre 40 colonne (totale 44) secondo la formula:

  $$W[i] = \begin{cases} W[i-4] \oplus W[i-1] & 4 \nmid i \\ W[i-4] \oplus T(W[i-1]) & 4 \mid i \end{cases}$$

  dove T è la trasformazione non lineare della S-box (resistenza a crittoanalisi lineare).

  La chiave k_i per la fase $i \in \{1, \dots, 10\}$ è data dalle colonne $W[4i], \dots, W[4i+3]$ (non si usa direttamente k come chiave di fase)

Ciascuna delle 10 fasi ha la seguente struttura:

substitute bytes B viene trasformato mediante la S-box;

shift rows i byte di ogni riga r (contando da 0) vengono shiftati a sinistra di r posizioni (dispersione del contenuto di ogni colonna sulle altre);

mix columns (eccetto fase 10) trasformazione lineare di ogni B tramite prodotto di ciascuna colonna per una matrice M, scelta in modo che ogni byte del risultato dipenda da tutti i byte della colonna (operazioni in $\mathbb{F}_{2^8}$: prodotto mod 2^8, somma mod 2);

add round key $B \oplus k_i$.

I passi di shift rows e mix columns garantiscono diffusione totale già dopo 2 round.

La S-box è divisa in 16 sottofunzioni (una per byte), con le seguenti caratteristiche:

- calcolate tramite una tabelle 16×16 byte che contengono una permutazione di tutti i 256 interi a 8 bit: i primi 4 bit indicano la riga, gli altri 4 la colonna;
- a differenza di AES, non comprimono (tanti input quanti output) e sono definite anche algebricamente: ogni byte è sostituito con il suo inverso moltiplicativo in $\mathbb{F}_{2^8}$ (da qui la non linearità), moltiplicato per una matrice 8×8 bit e sommato ad un vettore colonna.

Un byte in $\mathbb{F}_{2^8}$ si può intepretare come i coefficienti di un polinomio di grado 8.