Cifrari a blocchi

RSA, DES, AES, ...
Aggiungiamo padding ai messaggi che non hanno lunghezza multipla della dimensione del blocco.

Problema:

- blocchi uguali nel messaggio producono blocchi cifrati uguali;
- poca diffusione;
- periodicità nel crittogramma sfruttabile nella crittoanalisi.

Soluzione: si compongono i blocchi da loro.

Cipher Block Chaining (CBC)

Indicato con m_i/c_i l'i-esimo blocco,

$$c_i = C(m_i \oplus c_{i-1}, k)$$

La sequenza iniziale c_0 per il primo XOR può essere scelta arbitrariamente (e.g. la data) e scambiata in chiaro.

Per decifrare:

$$m_i = c_{i-1} \oplus D(c_i, k)$$

si può parallelizzare perché serve il *crittogramma* (non il messaggio decifrato) precedente. Un altro vantaggio di usare solo il crittogramma per il chaining è che un crittogramma corrotto impedisce la decifrazione del blocco corrispondente e di quello successivo, ma non di altri.