Framework di Cifratura

Da un punto di vista ad alto livello, esistono diversi **Framework** (paradigmi di implementazione delle librerie) crittografici. Ogni framework ha diverse caratteristiche strutturali, aspetto sopratutto a quanto la libreria nasconde all'utente elementi a basso livello del protocollo di cifratura.

~~Framework Deterministico~~

Framework Probabilistico

Molti dettagli implementativi sono nascosti all'utente (ad esempio il vettore di un IV). Garantisce che, usando costante l'input, l'output cambia senza bisogno di azioni da parte dell'utente.

Framework Deterministico

Il mittente deve occuparsi di fornire gli elementi necessari ad assicurare che la funzione non fornisca output deterministici.
Il mittente deve quindi fornire anche il nonce e l'IV.
Gli schemi probabilistici quindi incapsulano uno schema deterministico.
I framework probabilistici inoltre gli IV/nonce vengono sempre generati CASUALMENTE

Framework AEAD (Authenticated Encryption with Associated Data)

Oltre agli input di un framework deterministico (chiave, plain text, nonce/IV) si richiedono anche gli ASSOCIATED DATA i quali non sono ne criptografati ne inclusi nel ciphertext.
Gli associated data quindi sono dati di cui viene garantita l'autenticità ma non la confidenzialità.
Questo fa si che la decifratura fallisca se i dati autenticati sono stati manomessi.
Questo consente di inviare in modo sicuro i metadati.