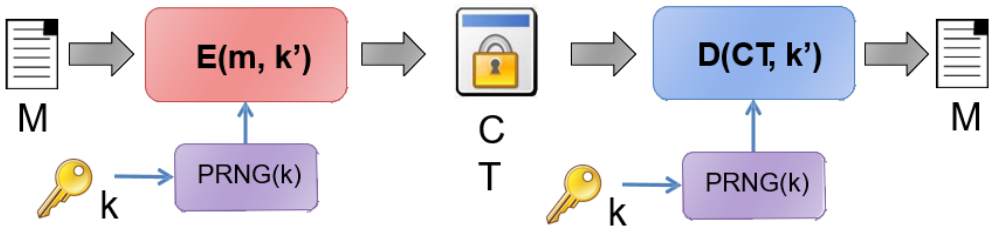
Stream Cipher e Vulnerabilità WEP

Introduzione alle Stream Cipher



Gli algoritmi di cifratura si dividono principalmente in due categorie: *cifrari a blocchi* e *cifrari a flusso* (stream cipher). I cifrari a flusso come RC4 (storicamente molto utilizzato, ma oggi considerato insicuro) e quelli moderni come Salsa20 e ChaCha20 sono progettati per cifrare i dati un byte per volta, generando una sequenza di bit pseudo-casuali chiamata *keystream*.

Le cifrature basate su blocchi come AES possono essere adattate per funzionare in modalità a flusso (ad es. AES-CTR), estendendo la loro flessibilità d'uso.

Funzionamento dei Cifrari a Flusso

Lo scopo ultimo della stream cipher è emulare idealmente un *One Time Pad*—dove il keystream è completamente casuale—ma, nella pratica, il keystream viene generato da un algoritmo deterministico basato su un seme segreto (tipicamente la chiave cifrante e un vettore di inizializzazione, IV).

Esistono due concetti da non confondere:

- **Chiave (Key):** segreta e condivisa fra mittente e destinatario.
- **Keystream:** sequenza pseudo-casuale, diversa per ogni messaggio, usata tramite operazione di XOR per cifrare e decifrare i dati.

La cifratura e la decifratura avvengono con l'operazione XOR tra il messaggio originale e il keystream. Tuttavia, se si usano la stessa chiave e IV per due messaggi diversi, il keystream e quindi il cifrato si ripetono, rendendo fragile la sicurezza.

➔ENC and DEC based on XOR (exactly as OTP)

➔CT = ENC(K, M) = M ⊕ keystream = M ⊕ PRNG(K)

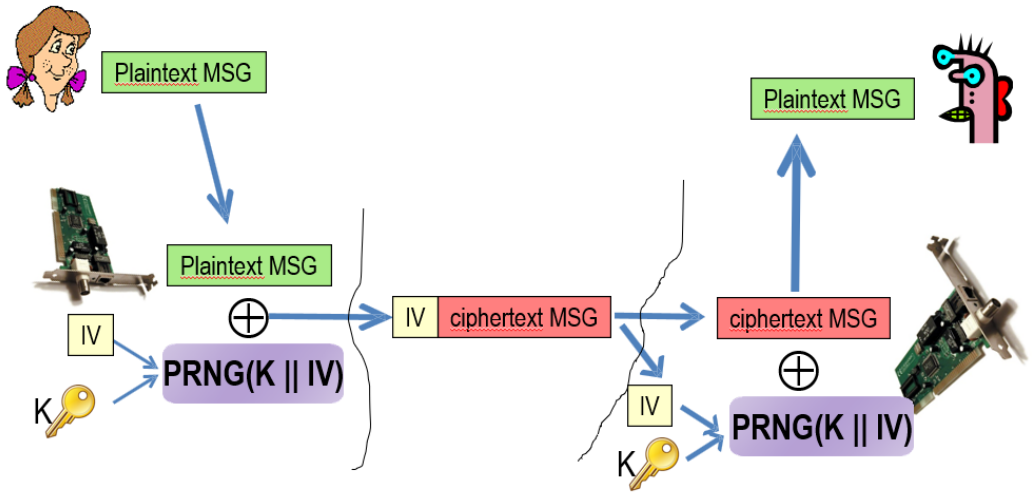
➔M = DEC(K, CT) = CT ⊕ keystream = CT ⊕ PRNG(K)

➔If substring repeats, ciphertext changes (good!)

➔

C	I	A	O		C	I	A	O		C	I	A	O	⊕
1	3	4	f		2	5	9	5		8	d	d	1	=
α	β	η	δ		φ	ϕ	τ	κ		σ	δ	λ	λ	

Sicurezza e Ruolo dell'Initialization Vector (IV)



Per assicurare la sicurezza semantica (cioè che lo stesso messaggio, cifrato più volte, dia sempre risultati diversi), ad ogni nuovo messaggio viene generato un nuovo IV. L'IV deve essere **fresco** e mai riutilizzato: la sua ripetizione compromette la sicurezza.

L'IV viene normalmente trasmesso in chiaro insieme al testo cifrato: la segretezza dell'algoritmo e del keystream non ne risente, purché la chiave rimanga privata e l'IV sia unico per ogni messaggio.

Il Caso WEP: Progettare Male Un Protocollo

Una lezione cruciale della sicurezza reale è che anche una buona cifra—come RC4 all'epoca—può essere totalmente insicura se usata con un protocollo mal progettato. WEP (Wired Equivalent Privacy), il primo standard per la sicurezza Wi-Fi, è un caso paradigmatico di errori progettuali.

Obiettivi WEP:

- Autenticazione degli utenti (in realtà troppo debole).
- Integrità dei messaggi (meccanismo inconsistente e facilmente aggirabile).
- Riservatezza dei dati (rottura dimostrata, anche a causa di errori sul protocollo e su RC4).

➔RC4 encryption:

⇨ENC(KEY,MSG) = MSG ⊕ RC4(IV, KEY)

⇨Keystream = RC4(IV, KEY)

Dettagli Tecnici e Errori di WEP

WEP genera il keystream tramite RC4 prendendo in input sia la chiave sia l'IV (24 bit). L'IV, piccolo e gestito malamente, viene spesso riutilizzato. Tali ripetizioni permettono facili attacchi—anche senza conoscere la chiave—grazie a tecniche di *known plaintext attack* (KPA) e *chosen plaintext attack* (CPA).

Problemi principali di WEP:

- IV troppo corto (24 bit): dopo poche ore di traffico il ciclo si esaurisce e gli IV si riutilizzano.
- L'IV viene lasciato gestire dal firmware/hardware senza linee guida: spesso parte da zero a ogni riavvio.
- È possibile costruire dizionari di keystream osservando traffico noto.
- L'integrità affidata a CRC32, funzione lineare e modificabile facilmente durante l'attacco.

Attacchi Pratici e Evoluzione Wi-Fi

Attacchi concreti (ad esempio quello di Fluhrer, Mantin e Shamir) sfruttano la debolezza dell'IV per estrapolare la chiave RC4, anche in presenza di chiavi lunghe. Successivi aggiornamenti degli standard Wi-Fi hanno introdotto WPA, WPA2 (nuove modalità e chiavi effimere, cifrari AES) e WPA3, che risolvono molti problemi ma sono sempre oggetto di attenzione (esempio: attacco KRACK nel 2017).

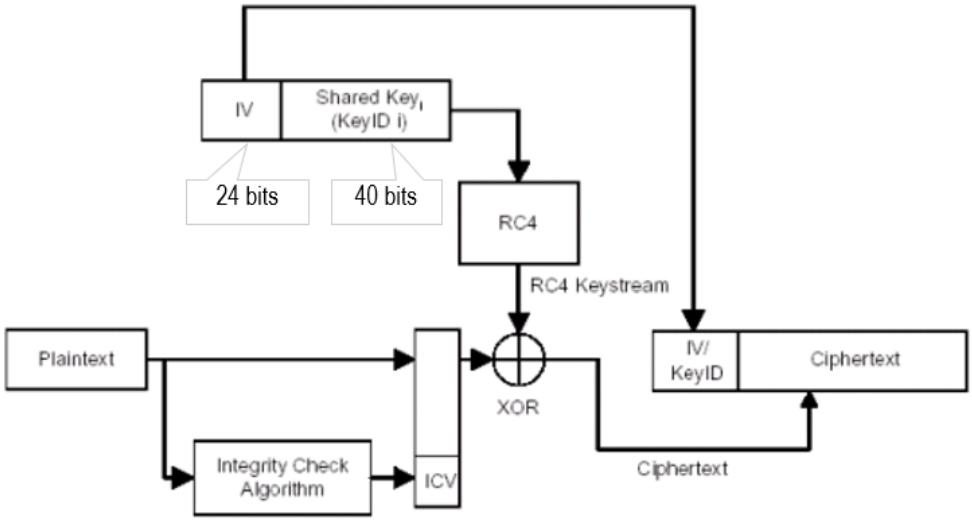
Meccanismi di Autenticazione

L'autenticazione consiste nel dimostrare di conoscere un segreto. Esistono diversi modi:

- Qualcosa che solo l'utente conosce (password, PIN).
- Qualcosa che solo l'utente possiede (token, smartcard, hardware biometrico).
- Qualcosa che rappresenta l'utente (biometria: impronte, riconoscimento facciale, comportamento, ecc.).
- Altri parametri contestuali (posizione, orari d'uso, ecc.).

WEP e la Debolezza dell'Autenticazione

WEP utilizza lo stesso segreto condiviso sia per la cifratura che per l'autenticazione (via challenge handshake): pur sembrando plausibile, questo apre a numerosi attacchi di replay, dizionario e impersonificazione. Basta infatti registrare un solo messaggio di autenticazione (IV e cifrato della challenge), per poter generare richieste illecite future.



Lezioni Chiave

- Un IV deve essere sempre unico e mai riutilizzato.
- L'integrità dei messaggi deve essere protetta da un meccanismo crittografico robusto, non da funzioni lineari come il CRC32.
- L'autenticazione non deve essere costruita semplicemente sulla rivelazione del segreto, ma su dimostrazioni che non rivelano la chiave originale.
- L'aggiornamento costante degli standard di sicurezza è fondamentale per prevenire nuove vulnerabilità.

Evoluzione degli Standard Wi-Fi

Oggi quasi tutte le reti utilizzano WPA2 o WPA3, con cifrari più robusti (AES), IV più lunghi e protocolli migliorati per chiavi effimere e autenticazione dell'utente.