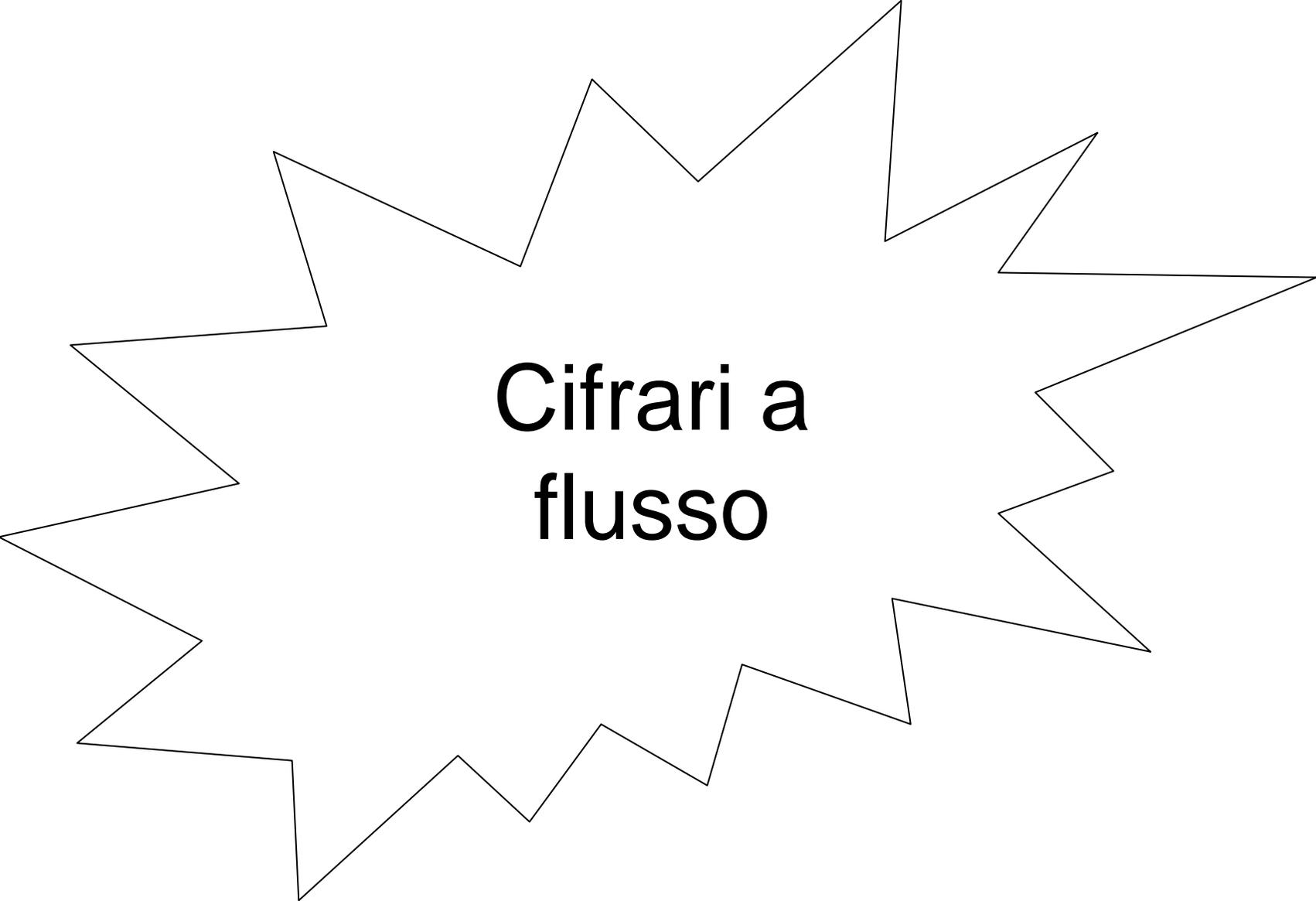


Cifrari simmetrici

Sicurezza dell'Informazione M
A.A. 2011 - 2012

Anna Riccioni
anna.riccioni@unibo.it



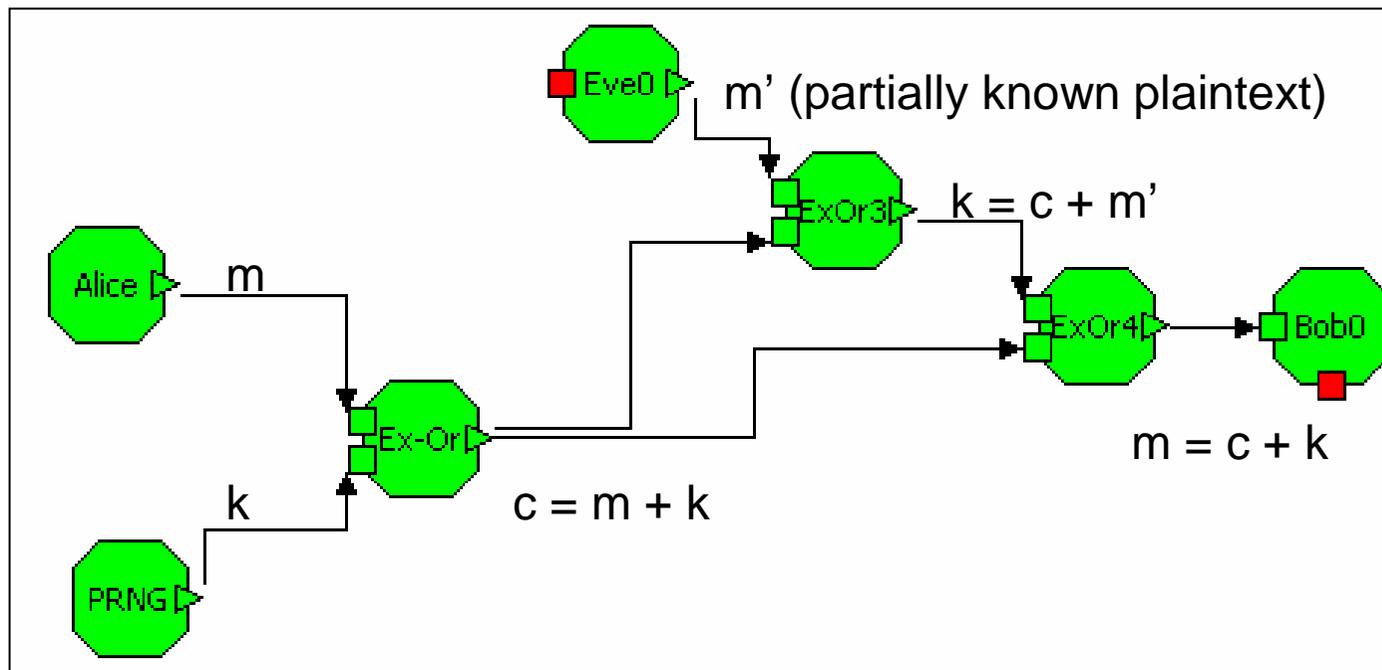
Cifrari a flusso

Vulnerabilità dei cifrari a flusso

Attacchi	Flusso sincrono	Autosincronizz.
Cancellazione di bit	Perdita di sincronismo	Transitorio
Inserzione di bit	Perdita di sincronismo	Transitorio
Modifica di bit	Non propagazione	Transitorio

Vulnerabilità dei cifrari a flusso

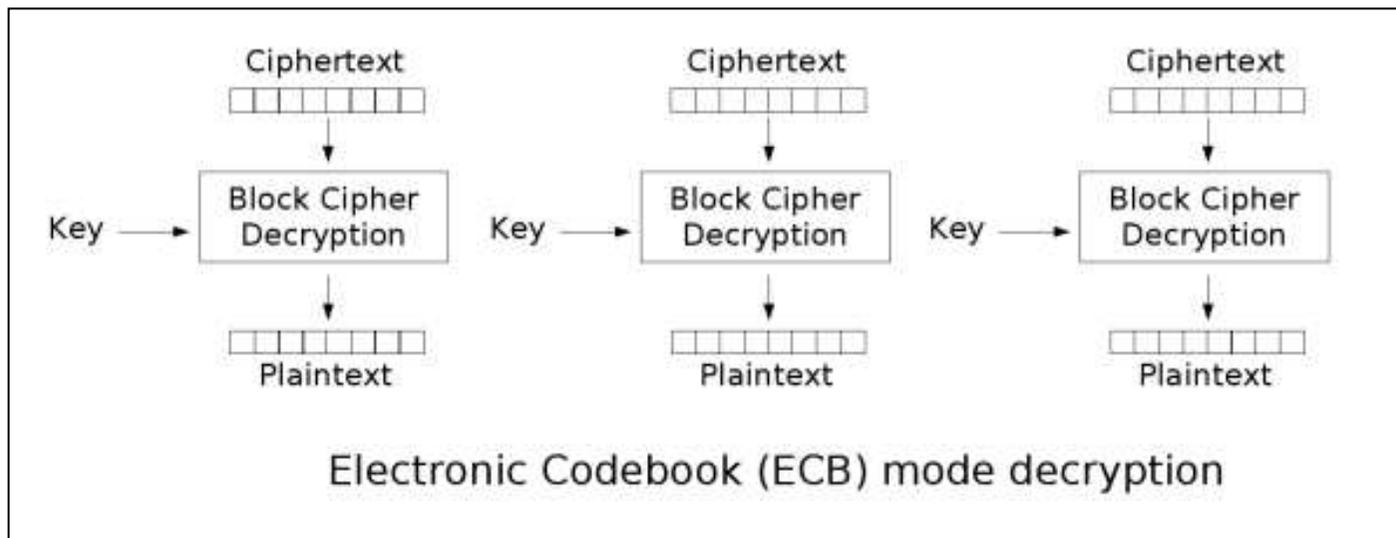
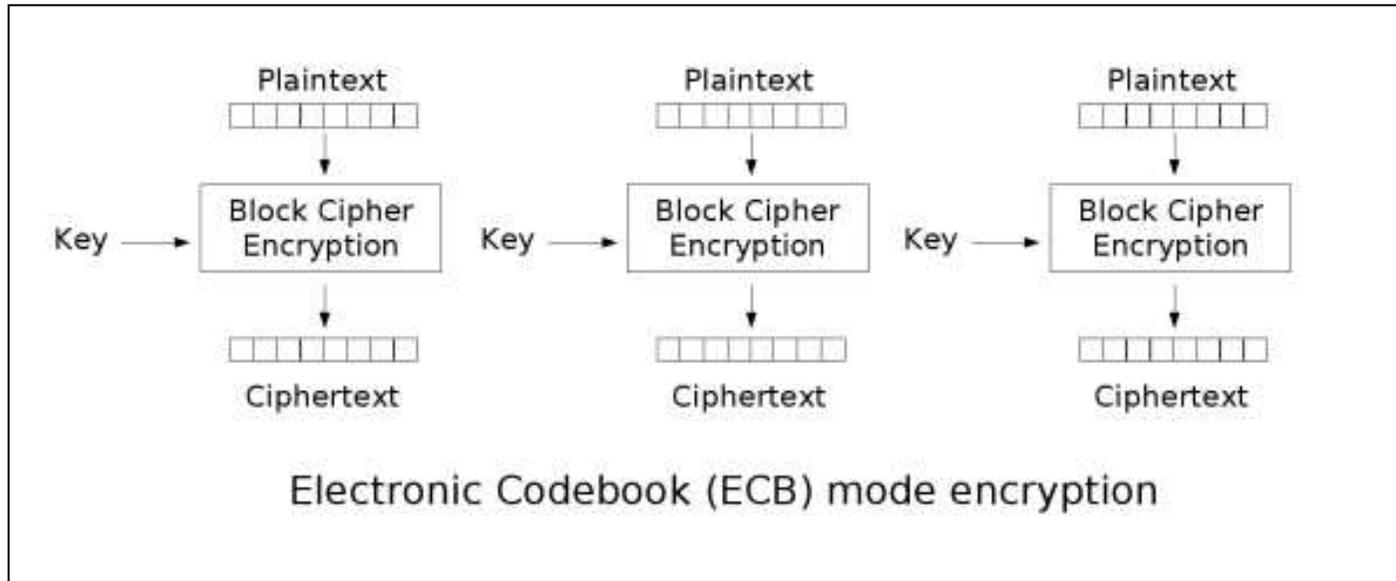
- XOR stream cipher
 - Ripetizione del flusso di chiave
 - Attacco con testo in chiaro noto
 - Combinazione dei due





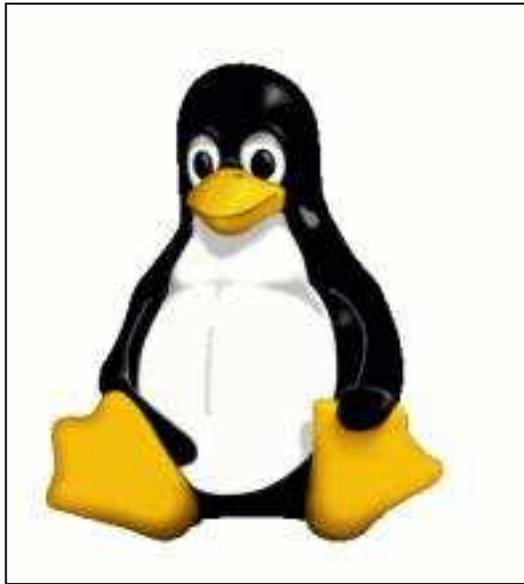
Cifrari a blocchi

Modalità operativa: ECB

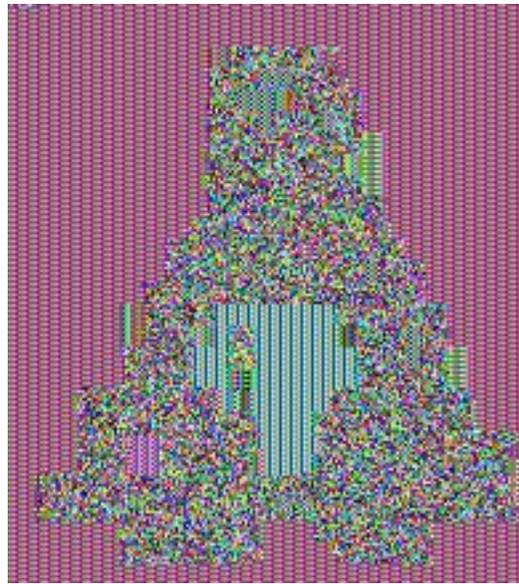


Fonte img:
Wikipedia

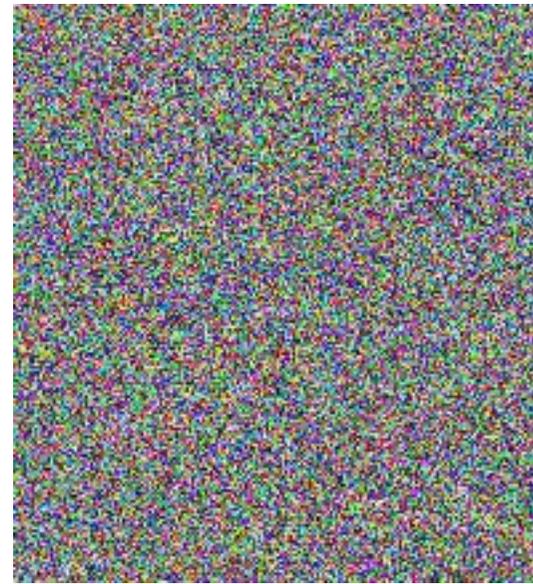
ECB drawbacks (S-vLab)



Originale



Cifrato in
modalità ECB



Cifrato in
modalità OFB8

Cifrare immagini in S-vLab (1/3)

- All'interno di S-vLab, i dati utilizzati in operazioni di cifratura e decifrazione vanno rappresentati mediante **array di byte**
 - quando si opera su **file**, l'intero contenuto del file (incluso l'**header** in cui è specificato il formato e altri metadati) viene trasformato in array di byte
 - una volta che un file è stato **cifrato** con S-vLab non è più possibile risalire al suo formato; anche un tentativo di aprire il file cifrato con il programma corretto (ad esempio, un editor di immagini se il file di partenza era un'immagine) non andrà a buon fine: il file sarà considerato corrotto

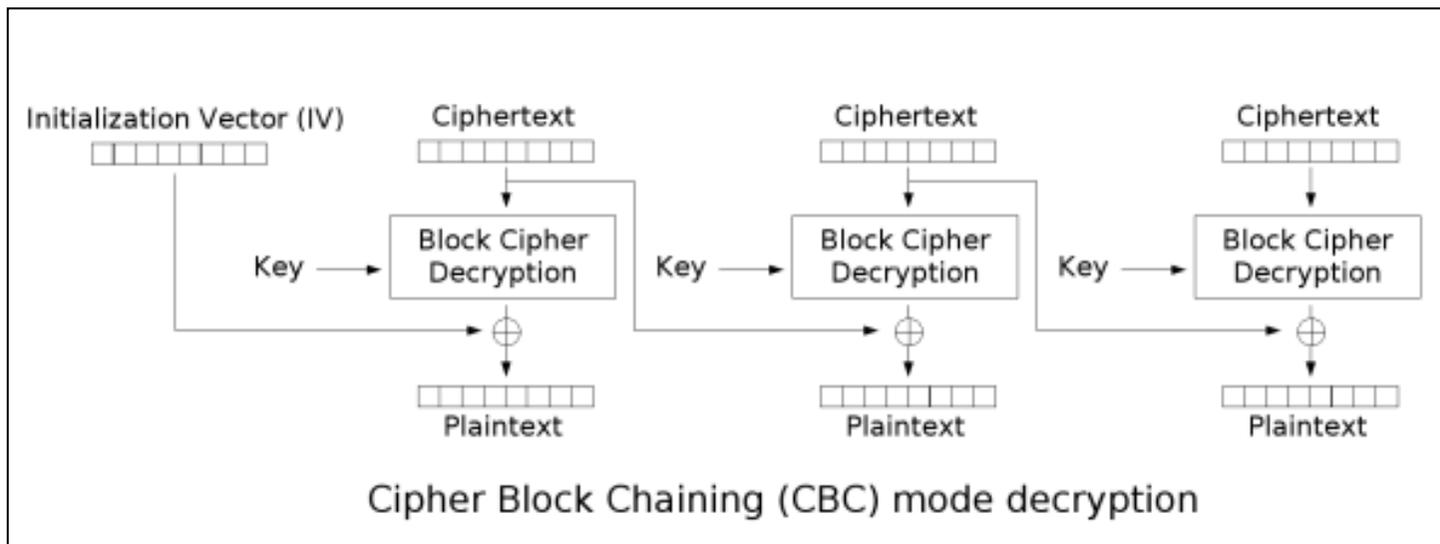
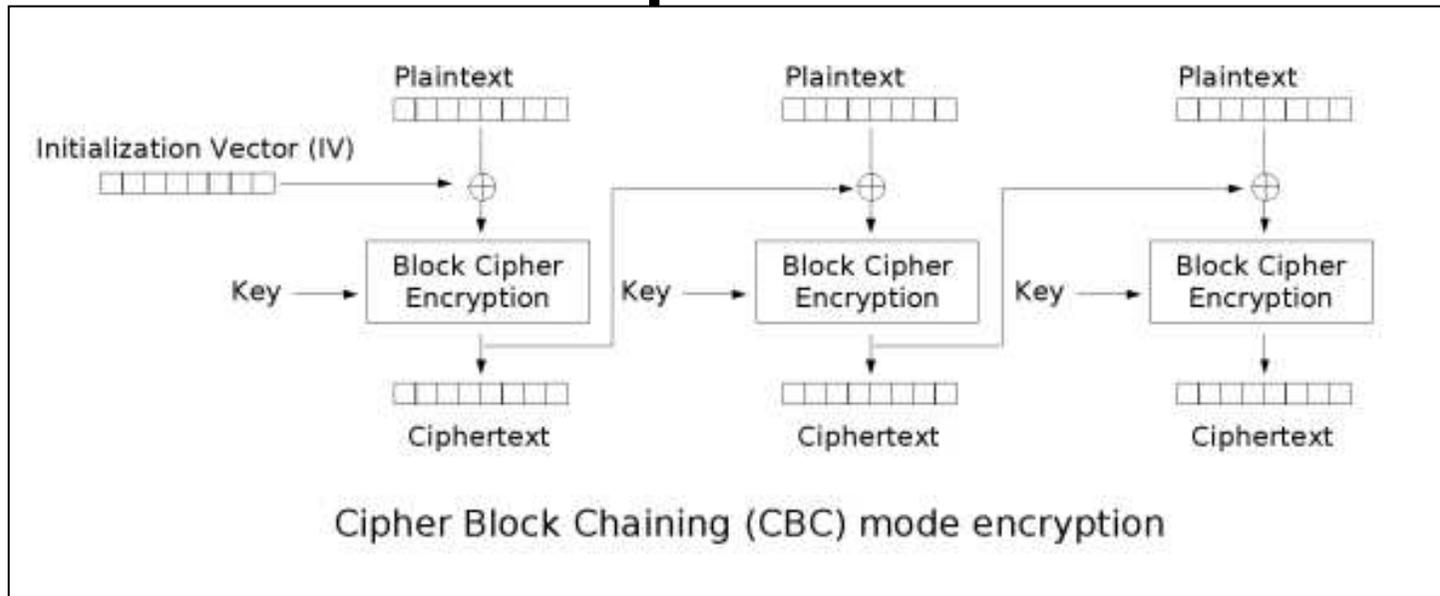
Cifrare immagini in S-vLab (2/3)

- Una corretta **decifrazione** del file ripristina interamente il suo contenuto
 - una volta che il file è stato correttamente decifrato, anche il suo **header** verrà ripristinato e sarà nuovamente possibile aprirlo ricorrendo agli opportuni programmi
- Se si vuole comunque aprire e visualizzare con un programma esterno un file cifrato occorre editarlo (con un editor per file binari) e sostituire l'header cifrato con il corrispondente header in chiaro

Cifrare immagini in S-vLab (3/3)

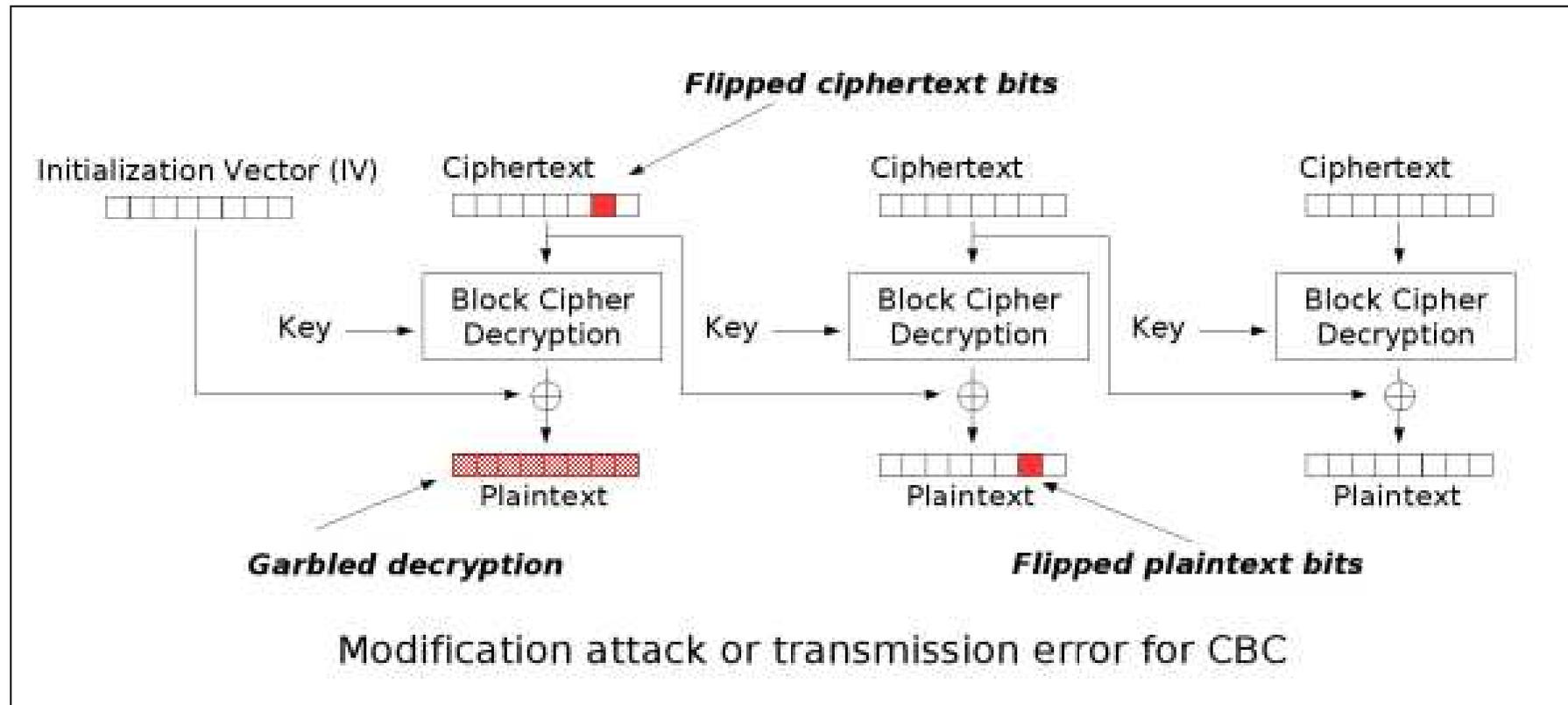
- Per riprodurre l'esperimento di cifratura di immagini:
 - il formato **ppm** è particolarmente indicato
 - ridondante e non compresso
 - header ridotto (specifiche disponibili sul sito:
<http://local.wasp.uwa.edu.au/~pbourke/dataformats/ppm/>)
 - un file ppm può essere importato attraverso il componente Alice in un qualunque schema all'interno di S-vLab (impostando una codifica binaria) e successivamente cifrato
 - il file cifrato può essere salvato tramite il componente Bob (specificando una codifica binaria e l'estensione .ppm)
 - il programma Cygnus Hex Editor permette di visualizzare l'header dell'immagine originale (in chiaro), di copiarlo e di incollarlo in testa al file cifrato: questo permette di aprire l'immagine cifrata con qualunque editor di immagini
 - download di una versione gratuita di Cygnus Hex Editor:
<http://www.softcircuits.com/cygnus/fe/>

Modalità operative: CBC

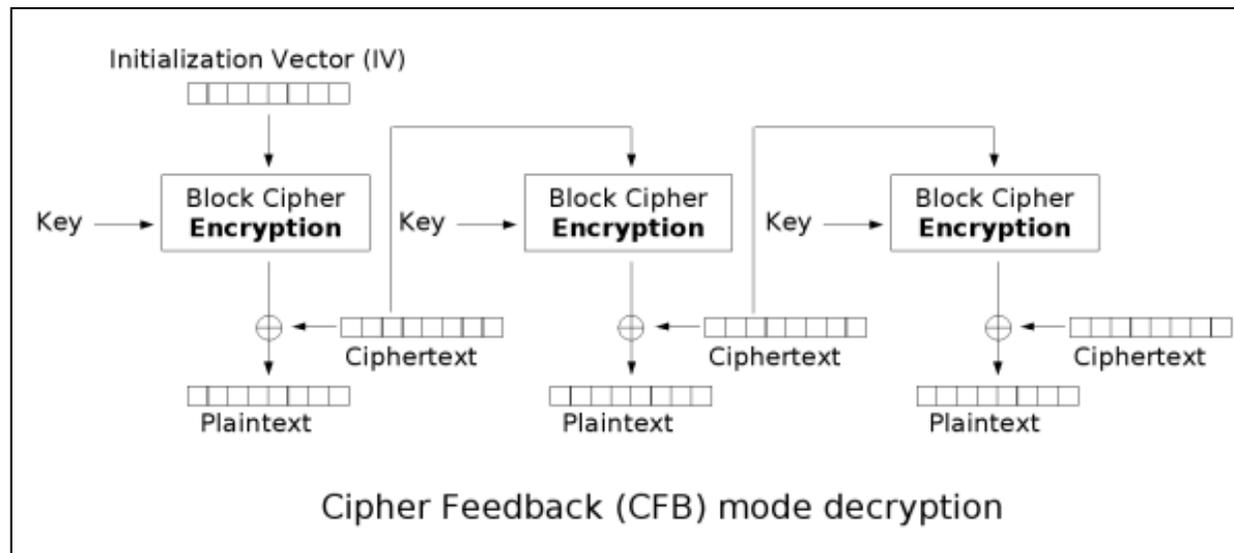
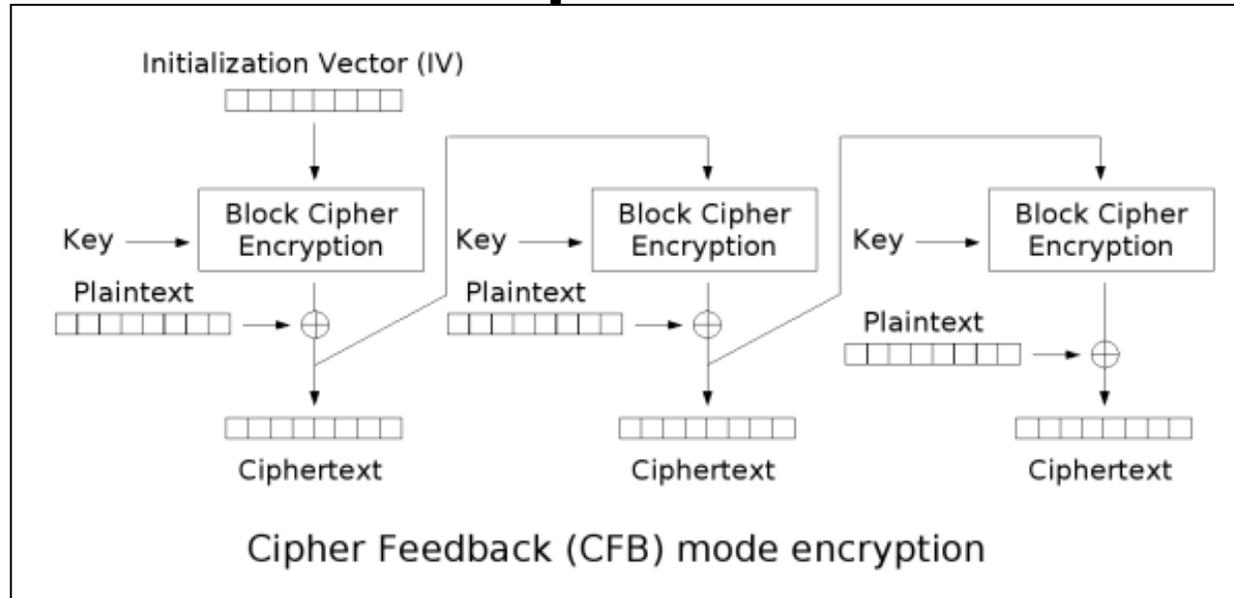


Fonte img:
Wikipedia

Propagazione degli errori

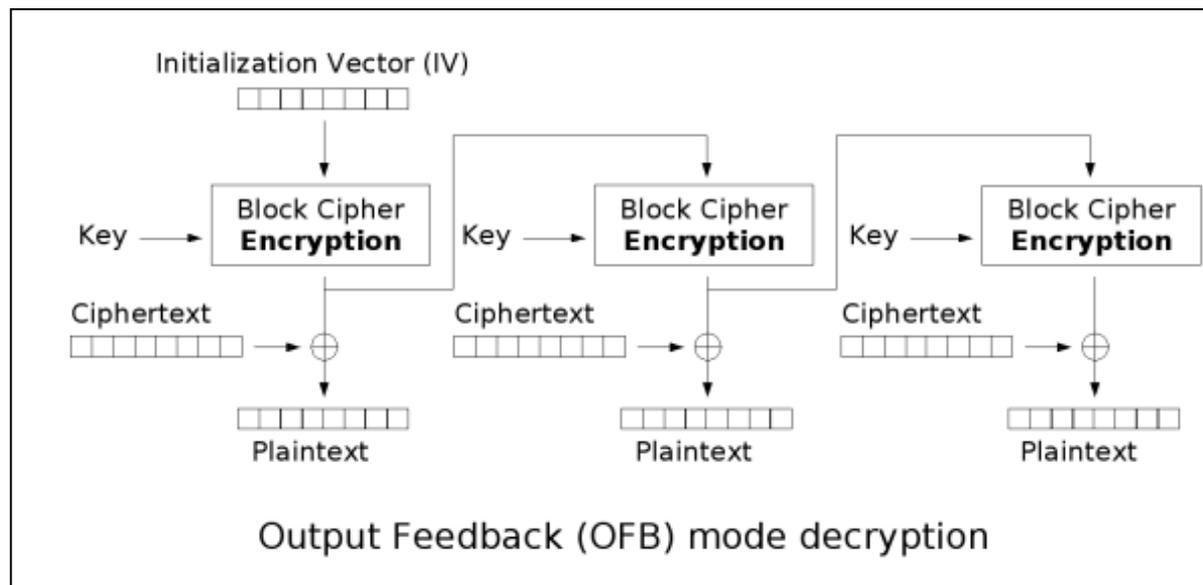
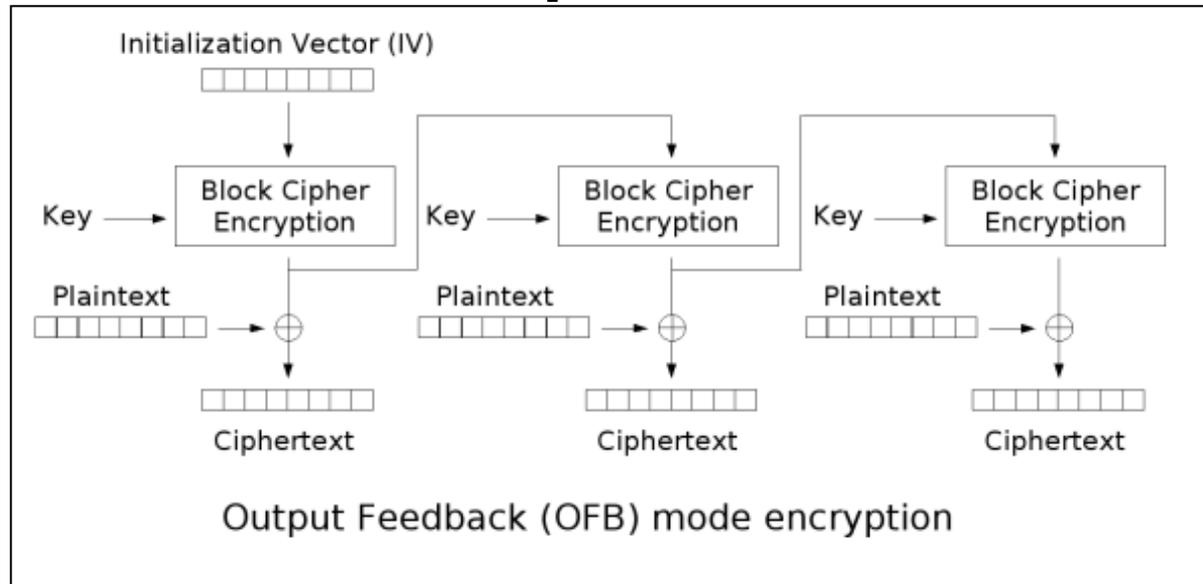


Modalità operativa: CFB



Fonte img:
Wikipedia

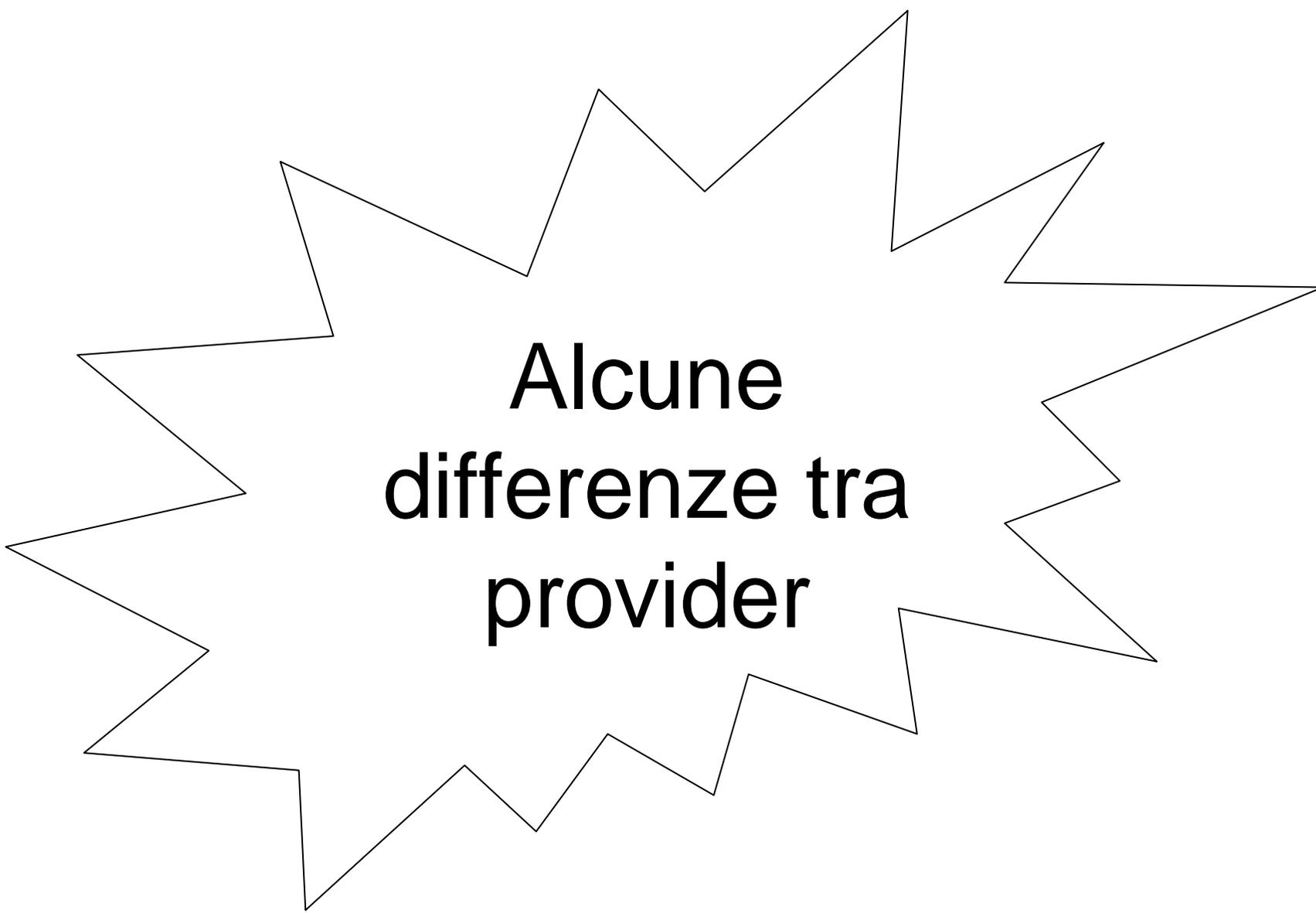
Modalità operativa: OFB



Fonte img:
Wikipedia

Esperimenti aggiuntivi in S-vLab sulle modalità operative

- Propagazione degli errori
 - Confrontare la propagazione di errori (simulando un attacco attivo) nelle varie modalità operative
- Simulazione di cifrari a flusso
 - Modificare la dimensione del blocco operativo di riferimento per le modalità OFB e CFB al fine di simulare un cifrario a flusso; valutare l'effetto sulla propagazione degli errori
- Efficienza
 - Confrontare i tempi di esecuzione in cifratura e decifrazione richiesti dalle varie modalità operative



**Alcune
differenze tra
provider**

Dimensione delle chiavi (1/2)

- Algoritmo DES
 - Quali valori di Key size sono accettati utilizzando il provider SunJCE?
 - Quali valori di Key size sono accettati utilizzando il provider BouncyCastle?
 - Qual è la dimensione finale della chiave generata utilizzando il provider BouncyCastle? C'è dipendenza dal parametro Key size?

Dimensione delle chiavi (2/2)

- Algoritmo TripleDES
 - Quali valori di Key size sono accettati utilizzando il provider SunJCE?
 - Qual è la dimensione finale della chiave generata utilizzando il provider SunJCE e specificando una key size di 112 bit? La chiave generata contiene qualche particolarità?
 - Quali valori di Key size sono accettati utilizzando il provider BouncyCastle?
 - Qual è la dimensione finale della chiave generata utilizzando il provider BouncyCastle e specificando una key size di 112 o di 128 bit?

S-vLab: sperimentazioni sulla dimensione delle chiavi (1/2)

- Istanziare un KeyGenerator e configurarlo in modo da generare:
 - una chiave da 56 bit per DES con SunJCE
 - qual è la dimensione della chiave generata?
 - una chiave da 64 bit per DES con SunJCE
 - una chiave da 10 bit per DES con SunJCE
 - una chiave da 56 bit per DES con BC
 - qual è la dimensione della chiave generata?
 - una chiave da 64 bit per DES con BC
 - qual è la dimensione della chiave generata?
 - una chiave da 10 bit per DES con BC
 - qual è la dimensione della chiave generata?

S-vLab: sperimentazioni sulla dimensione delle chiavi (2/2)

- Istanziare un KeyGenerator e configurarlo in modo da generare:
 - una chiave da 112 bit per TripleDES con SunJCE
 - qual è la dimensione della chiave generata? Che particolarità ha?
 - una chiave da 128 bit per TripleDES con SunJCE
 - una chiave da 168 bit per TripleDES con SunJCE
 - una chiave da 112 bit per TripleDES con BC
 - qual è la dimensione della chiave generata?
 - una chiave da 128 bit per TripleDES con BC
 - una chiave da 168 bit per TripleDES con BC
 - una chiave da 192 bit per TripleDES con BC

S-vLab: componente SecretKeyFactory

- Ci sono differenze nel suo funzionamento tra le implementazioni proposte dai due provider disponibili?