



UNIVERSITÀ DEGLI STUDI DI PERUGIA  
FACOLTÀ DI INGEGNERIA

## Appunti di Sicurezza Informatica

*Alessio Burani*  
*Silvia Cascianelli*

Anno Accademico 2014/2015

# Indice

<b>1</b>	<b>Introduzione alla sicurezza informatica</b>	<b>3</b>
1.1	Premessa	3
1.1.1	Definizione	3
1.2	Concetti fondamentali	3
1.2.1	Sistema informativo e informatico	3
1.2.2	Vulnerabilità, Minacce, Attacchi, Difesa	4
1.2.3	Sicurezza informatica: definizione classica e requisiti CIA	5
1.2.4	Requisiti AAA	7
1.2.5	Tipologie di Minacce e Attacchi	8
1.2.6	Principi della Sicurezza Informatica	9
1.3	Fondamenti di Crittografia	11
1.3.1	Terminologia e definizioni preliminari	11
1.3.2	Definizione formale di un sistema crittografico	11
1.3.3	Complessità computazionale	12
1.3.4	Algoritmo pubblico o segreto?	12
1.3.5	Attacchi a sistemi crittografici	12
1.3.6	Tipi di funzioni crittografiche	14
1.4	Modelli di controllo degli accessi (Access control models)	16
1.4.1	Matrice di controllo degli accessi	16
1.4.2	Liste di controllo degli accessi (Access Control List ACL)	16
1.4.3	Controllo degli accessi basato su liste di capacità (Capabilities Access Control CAC)	17
1.4.4	Controllo degli accessi basato sui ruoli (Role-Based Access Control RBAC)	18
<b>2</b>	<b>Secret Key Cryptography</b>	<b>20</b>
2.1	Introduzione	20
2.1.1	Impieghi crittografia a chiave segreta	20
2.1.2	Cifrari a blocchi e cifrari a flusso	23
2.2	Cifratura a blocchi	23
2.2.1	Introduzione e concetti generali	23
2.2.2	Sostituzione e Permutazione	24
2.2.3	Cifrario a blocchi – schema generale	24
2.2.4	Cifrario a blocchi – esempio	24
2.3	Data Encryption Standard - DES	24
2.3.1	Perché chiavi da 56 bit?	25
2.3.2	Violabilità e sicurezza di DES	26
2.3.3	Violabilità DES - esempio	26
2.3.4	Violabilità DES - cifratura multipla	26
2.3.5	DES - Struttura base	26
2.3.6	DES - Permutazioni dei dati	27
2.3.7	DES - Generazione chiavi di round	29
2.3.8	Un round di DES	30
2.3.9	Mangler Function	31

<b>3</b>	<b>Modes of Operation</b>	<b>33</b>
3.1	Introduzione . . . . .	33
3.2	Cifrare messaggi di grandi dimensioni . . . . .	33
3.2.1	Electronic Code Book (ECB) . . . . .	33
3.2.2	Cipher Block Chaining (CBC) . . . . .	35
3.2.3	Output FeedBack Mode (OFB) . . . . .	38
3.2.4	k-bit Output FeedBack Mode (k-OFB) . . . . .	39
3.2.5	Cipher FeedBack Mode (CFB) . . . . .	40
3.2.6	CounTeR Mode (CTR) . . . . .	41
3.2.7	Vantaggi e svantaggi di CTR . . . . .	41
3.3	Generare message authentication code(MAC) . . . . .	42
3.3.1	Residuo CBC . . . . .	42
3.3.2	Assicurare confidenzialità e autenticità . . . . .	43
3.4	Cifratura multipla DES . . . . .	45
3.4.1	Cifratura multipla EDE o 3DES . . . . .	45
3.4.2	EDE con CBC Outside/Inside . . . . .	46
<b>4</b>	<b>Funzioni Crittografiche di Hash</b>	<b>48</b>
4.1	Introduzione . . . . .	48
4.2	Esempio di Applicazioni . . . . .	49
4.3	Lunghezza di un messaggio di Digest . . . . .	50
4.4	Impieghi degli Algoritmi di Hash . . . . .	51
4.4.1	Message Digest per MAC . . . . .	51
4.4.2	Cifratura/Decifratura . . . . .	52
4.4.3	Algoritmi di cifratura come algoritmi di hash . . . . .	52
4.4.4	Hash di grandi messaggi con algoritmi di cifratura come hash . . . . .	53
4.4.5	Rainbow Tables (Opzionale) . . . . .	53

# Capitolo 1

## Introduzione alla sicurezza informatica

### 1.1 Premessa

#### 1.1.1 Definizione

Che cosa significa sicuro? La parola sicurezza e l'aggettivo sicuro vengono sempre associati a beni che si desidera proteggere da possibili danni, danneggiamenti, perdita, e via dicendo. In particolare un bene è al sicuro se è ben protetto, e la sua messa in sicurezza non deve impedirne l'utilizzo. Esistono molteplici definizioni di sicurezza informatica, ad esempio:

- Security is the degree of protection against danger, damage, loss, and criminal activity [?].
- Security is a form of protection where a separation is created between the assets and the threat [?].

La parola sicurezza deriva dal latino *sine cura*: senza preoccupazione. La sicurezza di un sistema può essere definita come la conoscenza del fatto che l'evoluzione del sistema non produrrà stati indesiderati. Le cause che possono minare la sicurezza sono molteplici e spesso non prevedibili, quindi non si può parlare di sicurezza in senso assoluto, ma solo relativo (*"L'unico computer sicuro è un computer spento"*).

**Trasversalità della tematica:** Le problematiche di sicurezza interessano molteplici campi (attività lavorative, vita domestica, hobby, giochi, sport, etc.). Di fatto, ogni settore della vita moderna ha delle implicazioni relative alla sicurezza. Il livello di sicurezza di un'organizzazione dipende dai livelli di sicurezza di tutti i suoi comparti/settori. Il livello di sicurezza di un sistema è determinato dal livello di sicurezza dal suo comparto meno sicuro (principio dell'anello debole).

### 1.2 Concetti fondamentali

#### 1.2.1 Sistema informativo e informatico

- Per sistema informativo (information system) di un'organizzazione si intende l'insieme delle informazioni prodotte ed elaborate e delle risorse umane, materiali e immateriali, coinvolte nel processo di elaborazione di tali informazioni
- Per sistema informatico (information and communication technology system) s'intende l'insieme delle varie tecnologie coinvolte nel sistema informativo (il sistema informativo è parte del sistema informatico).

Questo corso verterà sulla sicurezza dei sistemi informativi. Tuttavia, si approfondiranno maggiormente questioni inerenti la sicurezza dei sistemi informatici. Per sicurezza di un sistema

informativo si intende il grado di protezione contro qualsiasi minaccia ai suoi asset. Richiede il soddisfacimento dei seguenti requisiti:

- **confidenzialità, integrità e disponibilità**
- **assicurazione, autenticità e anonimato**

Quando si parla di **attacco** solitamente si intende la violazione di uno o più di questi requisiti.

### 1.2.2 Vulnerabilità, Minacce, Attacchi, Difesa

#### Vulnerabilità

Una vulnerabilità (o falla o breccia) è una **debolezza intrinseca** di un sistema, che potrebbe essere sfruttata per provocare perdite o danni. Scaturisce spesso da errate procedure di sicurezza e/o da errori di progettazione/implementazione, e in alcuni casi è intimamente legata alla natura del sistema. Ad esempio:

- un sistema potrebbe essere vulnerabile alla manipolazione non autorizzata dei dati causa un bug nella procedura di autenticazione dell'utente
- un calcolatore è vulnerabile all'acqua

Nel primo caso (vulnerabilità scaturite da errate procedure di sicurezza) l'insorgenza delle vulnerabilità può essere mitigata adottando adeguati standard e norme di qualità.

#### Minacce (Threats)

Per minaccia (threat) ad un sistema informatico/informativo si intende quell'insieme di circostanze che potrebbero arrecare danni ai suoi asset: eventi potenziali, accidentali o deliberati, che, nel caso accadessero, produrrebbero perdite e danni. Il realizzarsi di una minaccia generalmente avviene sfruttando una o più vulnerabilità del sistema. Si parla quindi di situazioni ipotetiche che potrebbero avvenire in determinate circostanze. Ad esempio:

- esecuzione di codice malevole che invia dati sensibili ad un'organizzazione criminale
- accesso a dati riservati da parte di entità non autorizzate
- perdita di dati a causa della rottura di un apparato hardware o al crash di uno specifico software

#### Attacchi (Attacks)

Un attacco (attack) è un atto deliberato teso ad arrecare un danno al sistema. Consiste, di fatto, nella realizzazione di una **minaccia**. Generalmente, un attacco viene perpetrato attraverso lo sfruttamento di una o più vulnerabilità. Spesso si classificano in base all'entità del danno:

- **attacco attivo (active attack)**: altera le risorse o ne modifica il processo di gestione/elaborazione
- **attacco passivo (passive attack)**: ottiene le informazioni/dati senza alterarli e senza modificare il relativo processo di gestione/elaborazione

Un'altra importante classificazione è in base "al luogo" da cui viene iniziato l'attacco:

- **attacco dall'interno (inside attack)**: attacco iniziato da un'entità all'interno del perimetro di sicurezza di un sistema informativo di una data organizzazione
- **attacco dall'esterno (outside attack)**: attacco iniziato da un'entità all'esterno del perimetro di sicurezza

Ovviamente, è molto più difficile prevenire e rilevare gli attacchi interni di quelli esterni. Ciò anche a causa del fatto che le misure di prevenzione per questo tipo di attacchi limita notevolmente l'usabilità del sistema (si pensi, ad esempio, alla struttura gerarchica in ambiente militare, in cui ogni risorsa conosce il minimo indispensabile per svolgere i propri compiti. In questo modo nel caso la risorsa venga compromessa, si limita il danno. Ovviamente tutto ciò rallenta il processo di funzionamento del sistema).

### Tecniche di difesa

Diverse contromisure (o misure protettive) possono essere attuate per proteggere un sistema informativo da eventi accidentali e da attacchi deliberati. Tali misure devono essere strutturate all'interno di un piano di sicurezza redatto dopo un'attenta analisi costi/benefici (textitcost-effective solutions). Le tecniche di difesa possono essere di tipo:

- **preventivo**: effettuano una serie di **controlli** per evitare **a priori** che attacchi noti o immaginabili possano essere sferrati con successo (e.g. controlli aeroportuali, controllo di accessi e permessi negli OS).
- **a posteriori**: sono tese a ridurre gli effetti di un attacco che è riuscito a eludere le misure preventive di cui sopra; devono monitorare un sistema ed essere in grado di **rivelare** comportamenti anomali.

Un **meccanismo di sicurezza** è un qualsiasi metodo, strumento, o procedura teso a rilevare, prevenire o porre rimedio agli effetti di un attacco alla sicurezza del sistema. La strategia di difesa, qualunque essa sia, combina in modo opportuno uno o più meccanismi di sicurezza. molti meccanismi di sicurezza consistono in controlli hardware/software.

### 1.2.3 Sicurezza informatica: definizione classica e requisiti CIA

La sicurezza informatica si fonda sulla protezione dei seguenti macro-requisiti di un sistema informativo (informatico):

- **Confidenzialità (Confidentiality)**
- **Integrità (Integrity)**
- **Disponibilità (Availability)**

Spesso si utilizza l'acronimo C.I.A. per denotarli in modo compatto. Ovviamente, come si può



Figura 1.1: Diagramma di Venn dei macro-requisiti di sicurezza

notare dal diagramma di Venn in Figura 1.1 spesso vengono richiesti contemporaneamente più di questi requisiti, così come un attacco può violare più requisiti.

### Confidenzialità (Confidentiality)

Def. **Confidentiality**: the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Per confidenzialità si intende quindi la garanzia che alle risorse informatiche accedano solo le parti autorizzate ad accedervi. E' talvolta denominata segretezza, riservatezza o privacy. Nota bene: per accesso non si intende solo la lettura, ma anche la visualizzazione, la stampa o la semplice consapevolezza dell'esistenza di una data risorsa nel sistema.

**Attacchi alla confidenzialità**: Si ha un attacco alla confidenzialità quando una entità (persona, processo o risorsa) tenta di accedere senza autorizzazione a informazioni protette (mentre queste sono memorizzate, oppure durante l'elaborazione, oppure ancora durante una comunicazione). La protezione della confidenzialità avviene utilizzando in modo appropriato i seguenti strumenti (meccanismi) di sicurezza informatica:

- **Cifratura (Encryption)**
- **Controllo degli accessi (Access Control)**
- **Sicurezza fisica (Physical security)**

### Integrità (Integrity)

Def. **Integrity**: safeguarding the accuracy and completeness of information and processing methods.

Def. **Integrity**: the property of safeguarding the accuracy and completeness of assets.

Per integrità si intende quindi la garanzia che le risorse possano essere modificate solo dalle parti autorizzate e solo nei modi prestabiliti. Le modifiche comprendono la scrittura, la variazione, il cambiamento dello stato, l'eliminazione e la creazione. Nel caso di file, conviene includere anche i metadati associati (proprietario, ultimo utente ad averlo letto, data ultima modifica, data di creazione), in modo che un accesso non autorizzato al contenuto possa essere rivelato da un controllo di integrità applicato ai metadati.

**Attacchi all'integrità**: Si ha un attacco all'integrità quando una entità (persona, processo o risorsa) tenta di modificare senza autorizzazione una o più risorse del sistema informativo.

La protezione della confidenzialità avviene utilizzando in modo appropriato i seguenti strumenti (meccanismi) di sicurezza informatica (tutti basati su un uso corretto della ridondanza):

- **Backup**
- **Somma di controllo o Checksum**
- **Codici a correzione di errore (Corruzioni non deliberate ma accidentali, possono essere facilmente elusi da attacchi intelligenti)**
- **Codici di autenticazione dei messaggi o Message Authentication Code MAC**

### Disponibilità (Availability)

Def. **Availability**: ensuring that authorized users have access to information and associated assets when required.

Per disponibilità (availability) si intende quindi che le risorse siano accessibili, nei tempi e nei modi prestabiliti, alle parti autorizzate ogni volta che le richiedono: se una persona o un sistema dispone dei diritti di accesso ad una risorsa, l'accesso non deve essergli impedito. Spesso la disponibilità viene citata tramite il suo opposto: la **negazione di servizio (Denial of Service o DoS)**. La disponibilità può assumere significati/sfumature diverse; una risorsa può trovarsi in uno stato intermedio tra i due opposti stati di piena disponibilità e di piena indisponibilità.

### Conflittualità requisiti CIA

Spesso i requisiti di confidenzialità, integrità e disponibilità possono essere in conflitto tra loro. E' quindi importante trovare il compromesso ottimo per la garanzia di tutti e tre. E' facile garantire la confidenzialità di una risorsa impedendo a chiunque di accedervi (e.g. se chiudo la risorsa in un blocco di cemento, sicuramente resterà confidenziale. Tuttavia la disponibilità della stessa verrebbe compromessa in senso assoluto).

#### 1.2.4 Requisiti AAA

In aggiunta ai concetti CIA, sovente viene richiesto il soddisfacimento di ulteriori requisiti che vanno sotto l'acronimo A.A.A.

##### Assicurazione (Assurance)

Per assicurazione (assurance) si intende come viene fornita e gestita la fiducia reciproca tra le varie parti coinvolte nel sistema informativo. Tale requisito sopperisce la mancanza di regolamentazione, da parte dei requisiti C.I.A., dell'uso delle risorse di un sistema. E' teso quindi ad evitare un uso non consono dei vari asset del sistema. Tale concetto è ovviamente bidirezionale: così come il sistema deve fidarsi degli utenti (del fatto che non lo usino in modo inappropriato), gli utenti devono fidarsi del sistema (e.g.:trattamento dei dati personali). Il concetto di fiducia è tuttavia difficile da quantificare ed è legato al grado di confidenza sul comportamento che ci si attende dal sistema. Il requisito di assicurazione viene regolato agendo sui seguenti strumenti:

- **Politiche (Policies):** specifiche comportamentali che regolano l'operato degli attori del sistema
- **Permessi (Permissions):** descrivono le operazioni ammesse/concesse e quelle proibite
- **Protezioni (Protections):** implementazione dei meccanismi di sicurezza tesi ad applicare e far rispettare le politiche e i permessi di cui sopra
- **Qualità del software:** lo sviluppo del software che rispetta standard di qualità rigorosi rende più difficile che il sistema si discosti dai comportamenti attesi

##### Autenticità (Authenticity)

L'autenticità è la capacità di provare che dichiarazioni, politiche e autorizzazioni rilasciate da persone o sistemi siano veritiere. Se non è garantita persone/sistemi possono sostenere argomentazioni non vere senza essere contraddetti da prove oggettive. Se è garantita, si dice anche che è soddisfatto il requisito del non-ripudio (non-ripudiation). Per non-ripudio si intende che dichiarazioni autentiche rilasciate da persone e/o sistemi NON possono essere negate. La firma digitale è il principale meccanismo crittografico che permette di ottenerlo. Un contesto in cui tale requisito è importante è, ad esempio, la PEC.

##### Anonimato (Anonymity)

Per anonimato (anonymity) si intende che non è possibile ottenere o risalire all'identità di un individuo pur avendo accesso a determinati record/transazioni di un sistema informativo. Se un'organizzazione deve rendere pubblici alcuni dati dei suoi clienti/membri senza violarne la privacy, può adottare alcuni dei seguenti strumenti:

- **Aggregazione (Aggregation):** combinare mediante somme e/o medie i dati di diversi individui
- **Miscelazione (Mixing):** permutare i dati dei singoli utenti in modo da preservare l'esito di predeterminate query
- **Mediazione (Proxies):** utilizzare degli agenti fidati che si interpongono tra l'individuo e i sistemi con i quali interagisce



- **Pseudonimi (Pseudonyms):** utilizzare delle identità fittizie eventualmente autenticate da una terza entità che funge da garante

### 1.2.5 Tipologie di Minacce e Attacchi

E' possibile classificare diverse minacce e attacchi rispetto a quali requisiti violano. Vediamone alcune:

#### Intercettazione (Eavesdropping)

Si ha un'intercettazione quando un'entità non autorizzata ha ottenuto l'accesso ad una risorsa. Generalmente questo tipo di attacchi avviene nella fase di trasmissione dell'informazione, e rappresenta una violazione alla confidenzialità. Esempi:

- copia illecita di file di programma o dati
- intercettazione di una comunicazione telefonica
- sniffing di pacchetti di dati

Un'intercettazione potrebbe essere molto difficile da rilevare, poiché un intercettatore "silenzioso" potrebbe essere molto abile e non lasciare tracce o cancellarle.

#### Alterazione (Alteration)

Si ha una alterazione o modifica quando un'entità non autorizzata, oltre ad accedere a una risorsa, interferisce con essa modificandola. Rappresenta una violazione alla confidenzialità. Esempi:

- attacchi di tipo **man-in-the-middle**: un flusso di dati viene intercettato, modificato e ritrasmesso (rappresenta anche una minaccia alla confidenzialità)
- virus informatici che modificano file di sistema critici in modo da eseguire azioni maliziose
- cambiare i valori di un database o modificare un programma in modo che esegua dei calcoli diversi

Alcuni casi di alterazione possono essere facilmente rilevati, mentre altre modifiche, più sottili, possono essere estremamente difficili da individuare.

#### Interruzione (Denial-of-service)

In un'interruzione, una risorsa del sistema viene degradata o eliminata, diventando non disponibile o inutilizzabile. Rappresenta una minaccia alla disponibilità e/o all'integrità. Esempi:

- la distruzione o il sabotaggio di un dispositivo
- la cancellazione di un file
- la congestione di un Web server causata da un numero enorme di richieste artificiali

#### Falsificazione (Masquerading)

La falsificazione consiste nella contraffazione di risorse (dati/hardware) da parti non autorizzate. Costituisce principalmente una violazione di autenticità, e a volte anche alla confidenzialità e/o all'integrità. Esempi:

- phishing: creazione di siti Web apparentemente identici agli originali allo scopo di frodare gli utenti
- textbfspoofing: spedizione di pacchetti dati con falsi indirizzi di ritorno

A volte le falsificazioni sono facilmente rilevabili, ma se attuate con abilità potrebbero essere del tutto indistinguibili da normali operazioni reali legittime.

**Ripudio (Ripudiation)**

Il ripudio consiste nel negare di aver effettuato una data azione. L'azione potrebbe essere la ricezione o la spedizione di un messaggio, così come l'esecuzione di una transazione. Spesso, riguarda il tentativo di recedere da un contratto (accordo) precedentemente assunto in cui era comunque previsto l'uso di ricevute (o simili) per dimostrare l'esecuzione di determinate operazioni. Si tratta di un attacco all'assicurazione.

**Inferenza (Inference), Correlation and traceback**

Per inferenza o attacco inferenziale si intendono un insieme di tecniche che utilizzando la statistica e l'algebra permettono di ricavare/stimare **informazioni sensibili** a partire da dati non sensibili. Rappresenta un attacco alla confidenzialità, e spesso è attuato nel contesto dei database. Similmente, per correlation and traceback si intendono un insieme di tecniche basate sulla statistica e sull'algebra che permettono di determinare la sorgente di una particolare informazione o di un particolare flusso di dati.

**N.B.:** C'è una differenza, in senso giuridico, tra dati personali e dati sensibili. Tale distinzione dipende dalla giurisdizione dei paesi. In particolare in Italia il dato personale viene indicato come un'informazione che permette di identificare un individuo (anagrafica), mentre un dato sensibile rappresenta un'informazione su aspetti della vita privata dell'individuo (orientamento sessuale, opinione politica, credo religioso, etc.)

**1.2.6 Principi della Sicurezza Informatica****Mediazione completa (Complete mediation):**

Ogni accesso ad una risorsa deve essere controllato verificando che sia conforme alle politiche di sicurezza stabilite; diffidare da miglioramenti nell'efficienza ottenuti salvando autorizzazioni precedentemente acquisite, poiché i permessi possono variare nel tempo.

**Struttura aperta (Open design):**

L'architettura, il progetto e l'implementazione dei meccanismi di sicurezza di un sistema devono essere resi pubblici.

- la sicurezza deve fondarsi sulla segretezza di pochi elementi chiave
- maggior feedback favoriscono l'individuazione di bug, falle e vulnerabilità, aumentando la robustezza e la sicurezza del sistema
- un meccanismo di protezione ritenuto sicuro da molti è preferibile ad uno noto solo a pochi. E' quindi bene evitare meccanismi di sicurezza basati sulla segretezza (security by obscurity).

**Separazione dei privilegi (Separation of privilege):**

Più condizioni dovrebbero essere richieste per concedere l'accesso a risorse limitate o ottenere il permesso di effettuare una data azione. In genere questo principio comporta una separazione logico/funzionale delle componenti di un sistema.

**Minimo privilegio (Least privilege):**

Ogni parte di un sistema deve avere i privilegi minimi necessari allo svolgimento dei propri compiti. Per attività inusuali che richiedono maggiori privilegi conviene assegnare autorizzazioni temporanee fortemente limitate nel tempo. In questo modo si riduce il rischio di attacchi basati sulla scalata di privilegi.

**Minimo meccanismo comune (Least common mechanism):**

I meccanismi di sicurezza che per l'accesso e la gestione di risorse condivise non dovrebbero essere a loro volta condivisi o dovrebbero essere condivisi il meno possibile. E' quindi buona norma adottare tecniche di isolamento quali la virtualizzazione e il sandboxing (e.g. browser web: nessuna applicazione web può agire sul filesystem, eccetto attraverso i cookies). In questo modo vengono mitigati rischi derivanti da comportamenti malevoli di utenti cui spetta comunque l'accesso a una data risorsa condivisa.

**Usabilità (Usability, Psychological acceptability):**

I meccanismi di sicurezza non devono rendere più difficile l'accesso alle risorse. Le interfacce utente devono essere ben progettate, intuitive e di facile utilizzo, mentre i parametri di configurazioni inerenti aspetti di sicurezza devono essere di semplice comprensione e facilmente modificabili.

**Fattore lavoro (Work factor):**

Il costo necessario ad aggirare un meccanismo di sicurezza deve essere confrontabile alle risorse di cui dispone un potenziale attaccante. Un meccanismo di sicurezza deve avere un livello di sofisticazione, e pertanto un costo, che tenga conto del valore degli asset da proteggere e delle risorse a disposizione di potenziali attaccanti.

**Monitoraggio (Compromise recording):**

A volte può convenire effettuare un monitoraggio dettagliato piuttosto che investire in sofisticati meccanismi di sicurezza di tipo preventivo.

**Penetrazione più semplice:**

un attaccante utilizzerà qualsiasi mezzo di penetrazione disponibile: non necessariamente i mezzi più ovvi (prevedibili), non necessariamente i mezzi per i quali sono state installate le difese più solide. (e.g.: E' inutile avere un sistema informatico sicuro se il personale non viene formato e fornisce a chiunque credenziali di accesso). L'applicazione di tale principio presenta le seguenti difficoltà:

- saper anticipare l'avversario, cioè riuscire a prevederlo
- gestire in modo equilibrato la sicurezza delle diverse parti di un sistema; rafforzare le difese di una parte può indurre gli avversari ad attaccare un'altra parte (più debole) del sistema.

**Temporalità:**

le risorse di un sistema informativo devono essere protette solo fino a quando possiedono un valore, e in modo proporzionale al loro valore. Generalmente tale principio si riferisce ai dati: il loro valore può subire brusche variazioni; si consideri ad esempio il valore dei dati sull'andamento dei mercati prima e dopo la loro divulgazione.

**Anello più debole:**

la sicurezza di un sistema articolato NON può essere più forte del suo anello più debole. La gestione della sicurezza deve tener conto del sistema nel suo insieme. Un elevato grado di sicurezza delle singole parti non implica un elevato grado di sicurezza globale, ma è necessario prevedere anche una strategia oculata di coordinamento della varie parti che non introduca vulnerabilità (l'insieme è più della somma delle parti).

## 1.3 Fondamenti di Crittografia

La parola Crittografia deriva dal greco, e significa "scrittura segreta". La crittografia è quindi l'arte e la scienza dello scrivere in modo segreto, ovvero l'arte di offuscare le informazioni in modo incomprensibile prevedendo una tecnica segreta per ricostruirle in modo esatto. L'applicazione storica della crittografia è la protezione della confidenzialità dei messaggi. Con **crittografia classica** si intende, infatti, l'insieme di tecniche che sopprimono la necessità di nascondere il contenuto di una comunicazione a soggetti non autorizzati. Con l'avvento dei calcolatori e del digitale, si è passati alla crittografia moderna, che presenta molte applicazioni aggiuntive di non immediata comprensione, ma estremamente utili:

- firma digitale
- controllo di integrità sicuro
- autenticazione

### 1.3.1 Terminologia e definizioni preliminari

- **Testo in chiaro (plaintext o cleartext):** messaggio nella sua forma originale
- **Testo cifrato (ciphertext):** messaggio cifrato (criptato o crittografato)
- **Cifratura o crittazione o criptazione (encryption):** processo che produce il testo cifrato a partire dal testo in chiaro
- **Decifratura o decrittazione o decryptazione (decryption):** processo inverso della cifratura
- **Crittografo (cryptographer):** esperto di crittografia
- **Crittoanalisi o crittanalisi (cryptanalysis):** l'arte o la scienza di violare testi cifrati; ricostruire il testo in chiaro senza disporre del segreto necessario alla fase di decifratura
- **Crittoanalista:** esperto di crittoanalisi
- **Crittologia (cryptology):** l'arte o la scienza delle scritture nascoste nella sua accezione più generale; include la crittografia e la crittoanalisi
- **Chiave segreta:** la segretezza dell'elaborazione nell'algoritmo è di solito concentrata nella segretezza di una chiave. E' stata introdotta perché è difficile concepire ogni volta nuovi algoritmi di cifratura ed è difficile spiegare rapidamente il funzionamento di un nuovo algoritmo ad un soggetto con il quale si desidera comunicare in modo sicuro

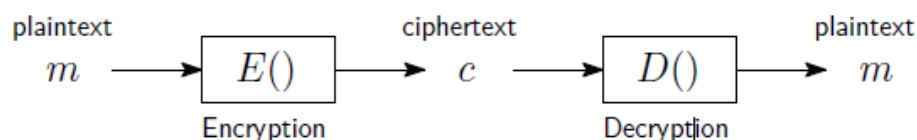


Figura 1.2: Schema a blocchi che illustra il processo cifratura-decifratura

### 1.3.2 Definizione formale di un sistema crittografico

: Formalmente, un sistema crittografico è costituito da sette componenti (a volte alcune di queste sono assenti o coincidono):

- l'insieme dei possibili input (plaintext)

- l'insieme dei possibili output (ciphertex)
- l'insieme delle possibili chiavi di cifratura
- l'insieme delle possibili chiavi di decifratura
- la corrispondenza tra chiavi di cifratura e di decifratura
- l'algoritmo di cifratura da usare
- l'algoritmo di decifratura da usare

### 1.3.3 Complessità computazionale

Uno schema crittografico anche assumendo che sia privo di vulnerabilità intrinseche, può essere (quasi) sempre sottoposto ad attacchi a forza bruta. Affinché ciò possa avvenire è necessario disporre di un test affidabile che permetta di dire se una chiave scelta a caso è quella corretta; cioè, essere in grado di riconoscere il testo in chiaro. Se tale condizione è verificata si può perseguire un approccio esaustivo in cui si tentano tutte le chiavi. Uno schema crittografico è allora tanto più sicuro quanto è maggiore il costo computazionale necessario a violarlo. Contemporaneamente deve garantire l'efficienza di cifratura/decifratura. Formalizzando, possiamo definire un sistema **computazionalmente sicuro** se:

- il costo per rendere inefficace il cifrario supera il valore dell'informazione cifrata
- il tempo richiesto per rendere inefficace il cifrario supera l'arco temporale in cui l'informazione ha una qualche utilità

Tuttavia, stimare lo sforzo computazionale richiesto per effettuare con successo la crittoanalisi del testo cifrato è molto difficile. Il tempo richiesto per un approccio a forza bruta fornisce soltanto un limite superiore: è realistico solo se l'algoritmo non presenta delle debolezze intrinseche di tipo matematico; in questo caso si possono effettuare stime ragionevoli su tempi e costi. In un approccio a forza bruta mediamente si devono provare metà di tutte le possibili chiavi. Ovviamente in questo processo prende parte, come variabile fondamentale, la lunghezza della chiave. Alcuni schemi crittografici prevedono una chiave avente lunghezza variabile: aumentandola aumenta la sicurezza, ma diminuisce l'efficienza. Altri schemi stabiliscono a priori la lunghezza della chiave, se si desidera aumentarla è necessario sviluppare algoritmi simili che utilizzano chiavi di lunghezza diversa, oppure è possibile combinare in modo opportuno tali schemi ottenendo uno schema risultante con una chiave globale più lunga (attenzione al modo in cui si combinano!).

### 1.3.4 Algoritmo pubblico o segreto?

Ottenere la sicurezza dalla segretezza cioè custodendo gelosamente e nascondendo la metodologia di cifratura/decifratura, **security by obscurity**, è assolutamente da evitare. Questo perché:

- mantenere la segretezza è difficile, poiché le tecniche di reverse engineering permettono di risalire al codice
- è una strategia in chiara opposizione al fundamental tenet of cryptography

Oggigiorno, nelle applicazioni di uso civile/commerciale si usano schemi crittografici di dominio pubblico. La segretezza, laddove prevista, è conseguenza di altre cause (e.g. protezione del segreto industriale, contesti militari).

### 1.3.5 Attacchi a sistemi crittografici

Si possono distinguere cinque categorie di attacchi in base al tipo di informazioni in possesso dell'attaccante (di cui gli ultimi due meno frequenti):

**Solo testo cifrato (ciphertext only)**

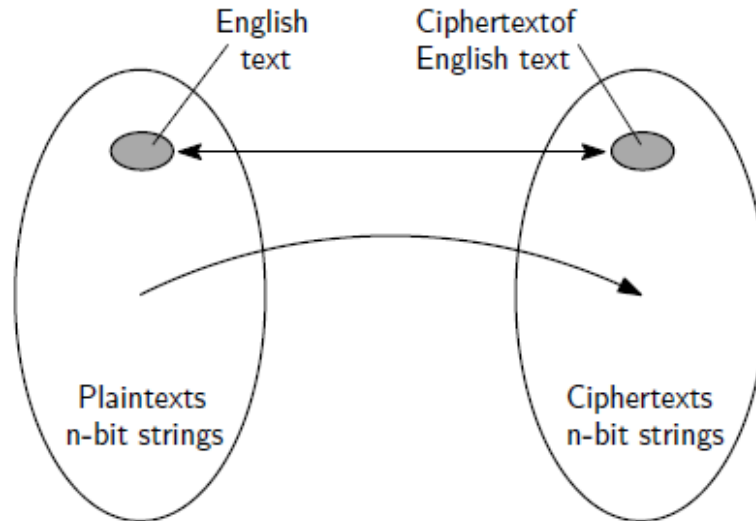
L'attaccante conosce l'algoritmo di cifratura e dispone soltanto di una certa quantità di testo cifrato. Nell'ipotesi che non vi siano vulnerabilità intrinseche nello schema crittografico, l'attaccante può tentare un attacco forza bruta, a patto che disponga di un test affidabile per il riconoscimento del testo in chiaro e di potenza di calcolo sufficiente. Tale attacco è anche noto come **testo in chiaro riconoscibile (recognizable plaintext)**. Riguardo la riconoscibilità del testo in chiaro valgono le seguenti osservazioni:

- nel caso di messaggi testuali, è molto improbabile che una chiave di decifratura errata permetta di ottenere un messaggio verosimile
- è essenziale avere una sufficiente quantità di testo in chiaro

**Esempio:** il messaggio  $m$  è una frase di un qualche linguaggio naturale. Ipotizzando che i caratteri di  $m$  siano codificati in ASCII a 8 bit e il testo cifrato  $c$  abbia la stessa lunghezza di  $m$  (quasi sempre è così). Siano:

- $t$ : il numero di caratteri di  $m$  e di  $c$
- $n = 8t$ : il numero di bit di  $m$  e di  $c$
- $2^{\alpha n}$ : il numero totale di messaggi distinti, nel linguaggio naturale considerato, di lunghezza  $n$  bit

Si osservi che nominalmente esistono  $2^n$  stringhe binarie di  $n$  bit, ma solo una piccolissima frazione di queste è la codifica di un messaggio nel linguaggio naturale,  $0 < \alpha < 1$  è un fattore correttivo usato per modellare tale fenomeno, per la lingua inglese  $\alpha = 0.16$ .



Il seguente rapporto:

$$\frac{2^{\alpha n}}{2^n} = \frac{1}{2^{(1-\alpha)n}} \quad (1.1)$$

rappresenta la probabilità che un stringa random di  $n$  bit costituisca la codifica di un messaggio nel linguaggio naturale considerato. Se la chiave di decifratura ha una lunghezza di  $k$  bit, effettuando un attacco a forza bruta ( $2^k$  tentativi), il numero atteso di messaggi verosimili (nel linguaggio naturale dato) associabili al testo cifrato  $c$  è pari a:

$$\frac{2^k}{2^{(1-\alpha)n}} \quad (1.2)$$

Essendo  $k$  fissato, al crescere di  $n$  tale numero tende rapidamente a zero, quindi il test di riconoscibilità diventa quasi infallibile se si dispone di una sufficiente quantità di testo cifrato. In alcuni casi, si potrebbe tentare un approccio a forza bruta computazionalmente meno costoso se:

- la chiave di decifratura coincide con quella di cifratura, spesso è così
- la chiave di cifratura 'e derivata da una password di utente segreta con una procedura nota (si può tentare un approccio a forza bruta sullo spazio delle password, sensibilmente più piccolo dello spazio delle chiavi)

**IMPORTANTE:** uno schema crittografico deve **SEMPRE** essere sicuro contro attacchi di tipo **ciphertext only**, poiché il testo cifrato è sempre facilmente intercettabile e ottenibile.

### Testo in chiaro conosciuto (known plaintext)

In questo caso, il crittoanalista conosce:

- l'algoritmo di cifratura
- un certo insieme di coppie  $\langle \textit{plaintext}, \textit{ciphertext} \rangle$ , ma non ha la facoltà di decidere lui il tipo specifico di plaintext
- una certa quantità di testo cifrato

Alcuni schemi crittografici potrebbero essere molto resistenti ad attacchi di tipo **ciphertext only** ma rivelarsi vulnerabili ad attacchi di tipo **known plaintext**. In caso di impiego, è fondamentale prevenire che un attaccante ottenga coppie  $\langle \textit{plaintext}, \textit{ciphertext} \rangle$ .

### Testo in chiaro selezionato (chosen plaintext)

In questo caso, il crittoanalista conosce:

- l'algoritmo di cifratura
- una certa quantità di testo cifrato (con chiave segreta  $K$ )

e può scegliere a piacimento il testo in chiaro ed ottenere il relativo testo cifrato (sempre con la chiave  $K$ ). In altre parole può scegliere quali coppie  $\langle \textit{plaintext}, \textit{ciphertext} \rangle$  conoscere. E' possibile che un sistema crittografico sia sicuro contro attacchi di tipo **ciphertext only** e **known plaintext**, ma sia vulnerabile ad attacchi di tipo **chosen plaintext**.

### Testo cifrato selezionato (chosen ciphertext)

L'attaccante dispone (oltre che dell'algoritmo di cifratura e del testo cifrato da decifrare) di testo cifrato, con significato, scelto da lui, e corrispondente testo in chiaro.

### Testo selezionato (chosen text)

L'attaccante dispone sia di testo in chiaro scelto da lui (e corrispondente testo cifrato) sia di testo cifrato scelto da lui (e corrispondente testo in chiaro).

## 1.3.6 Tipi di funzioni crittografiche

- funzioni a chiave pubblica (public key functions): richiedono l'uso di due chiavi, una pubblica e una privata (approfondire non ripudio su firma digitale)
- funzioni a chiave segreta (secret key functions): richiedono l'uso di una singola chiave
- funzioni hash (hash functions): non usano alcuna chiave

Tipologia di attacco	Informazioni in possesso al crittoanalista
<i>solo testo cifrato</i> ( <i>ciphertext only</i> )	<ul style="list-style-type: none"> <li>• algoritmo di cifratura</li> <li>• testo cifrato da decifrare</li> </ul>
<i>testo in chiaro conosciuto</i> ( <i>known plaintext</i> )	<ul style="list-style-type: none"> <li>• algoritmo di cifratura</li> <li>• testo cifrato da decifrare</li> <li>• uno o più testi in chiaro e corrispondenti testi cifrati</li> </ul>
<i>testo in chiaro selezionato</i> ( <i>chosen plaintext</i> )	<ul style="list-style-type: none"> <li>• algoritmo di cifratura</li> <li>• testo cifrato da decifrare</li> <li>• testo in chiaro scelto dal crittoanalista e relativo testo cifrato</li> </ul>
<i>testo cifrato selezionato</i> ( <i>chosen ciphertext</i> )	<ul style="list-style-type: none"> <li>• algoritmo di cifratura</li> <li>• testo cifrato da decifrare</li> <li>• testo cifrato, con significato, scelto dal crittoanalista e corrispondente testo in chiaro</li> </ul>
<i>testo selezionato</i> ( <i>chosen text</i> )	<ul style="list-style-type: none"> <li>• algoritmo di cifratura</li> <li>• testo cifrato da decifrare</li> <li>• testo in chiaro scelto dal crittoanalista e relativo testo cifrato</li> <li>• testo cifrato, con significato, scelto dal crittoanalista e corrispondente testo in chiaro</li> </ul>

Figura 1.3: Tabella riassuntiva tipologie di attacchi

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ $\mu$ s	Time required at $10^6$ decryptions/ $\mu$ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

Figura 1.4: Tempo medio per una ricerca esaustiva



## 1.4 Modelli di controllo degli accessi (Access control models)

Il controllo degli accessi alla varie risorse di un sistema informativo costituisce un fondamentale meccanismo di sicurezza di tipo **preventivo**. Previene attacchi alla confidenzialità, all'integrità e all'anonimato. L'idea di base è restringere l'accesso solo a coloro che hanno la necessità di accedere e/o modificare specifiche risorse, in accordo al principio del **minimo privilegio**.

### 1.4.1 Matrice di controllo degli accessi

Una matrice di controllo degli accessi (Access Control Matrix ACM) è una tabella che definisce i permessi di accesso dei vari **soggetti** di un sistema informativo ai suoi **oggetti**.

- un **soggetto** è un utente, un gruppo o una generica entità attiva che desidera effettuare una data azione su un data risorsa
- un **oggetto** è un file, un documento, un dispositivo, una generica risorsa o più in generale un'entità passiva sulla quale si desidera compiere una data azione

Ogni riga della tabella è associata ad un soggetto, e ogni colonna è associata ad un oggetto. Ogni cella stabilisce quindi il tipo di azione consentita; il soggetto e l'oggetto sono implicitamente definiti dalla cella. Diverse modalità di accesso sono possibili: lettura, scrittura, copia, esecuzione, cancellazione, annotazione. Una cella vuota stabilisce che non viene assegnato alcun tipo di accesso.

	/etc/passwd	/home/mario/	/admin/
root	read, write	read, write, exec	read, write, exec
pipito	read		
mario	read	read, write, exec	
backup	read	read, exec	read, exec
...	...	...	...

Figura 1.5: Esempio access control matrix

### Pro e Contro ACM

L'adozione di una ACM offre, in linea di principio, i seguenti vantaggi:

- immediatezza nel valutare e modificare i diritti di accesso per una data coppia soggetto-oggetto
- facilità di visualizzazione e gestione: semplifica la vita all'amministratore

Purtroppo, il grande svantaggio delle ACM, che ne limita fortemente l'applicabilità, è la mancanza di scalabilità. E' del tutto ragionevole pensare che un computer server possa avere ordine di  $10^3$  soggetti (per lo più utenti) e  $10^6$  oggetti (files e directories), richiedendo una ACM di  $10^9$  celle. In questi ordini di grandezza i precedenti vantaggi decadono (non scalabilità).

### 1.4.2 Liste di controllo degli accessi (Access Control List ACL)

Una lista di controllo degli accessi (access control list ACL) segue un approccio di tipo "object-centered" per garantire una buona scalabilità, in particolare:

- ad ogni oggetto **o** viene associata una lista **L**, detta la lista di accesso di **o**, che enumera tutti i soggetti che hanno un qualche diritto di accesso ad **o**, e

- per ciascuno di tali soggetti,  $s$ , sono specificati i tipi di azioni che  $s$  può compiere su textbfo

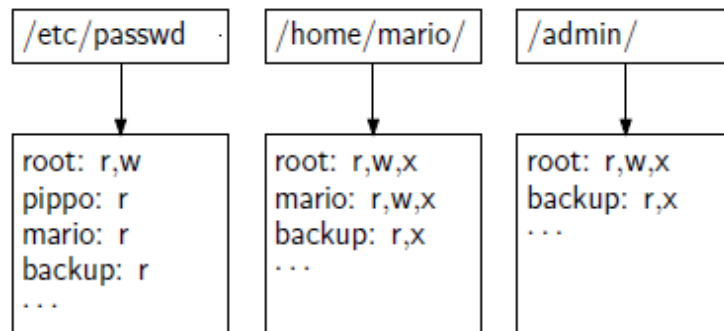


Figura 1.6: Esempio access control list

Nella pratica, il modello ACL comporta un significativo risparmio di memoria rispetto al modello ACM: ogni lista del modello ACL è ottenibile scandendo la relativa colonna del modello ACM ignorando però le celle vuote.

### Pro e Contro ACL

Il principale vantaggio del modello ACL rispetto al modello ACM è la minor occupazione di memoria che si registra nella pratica (in teoria, nel caso peggiore l'occupazione è la medesima). La memoria occupata complessivamente nel modello ACL,  $\sum_O size(L_O)$ , è proporzionale a  $C_{nv}(ACM)$  cioè al numero di celle non vuote della ACM. Nella pratica  $C_{nv}(ACM)$  è molto minore di  $C(ACM)$  (che denota il numero totale di celle della ACM); cioè nella pratica  $C_{nv}(ACM) \ll C(ACM)$ . Un altro vantaggio è la facilità di gestione delle ACL da parte del sistema operativo:

- sono incorporate nei metadati associati all'oggetto in questione (i.e. filesystem)
- per verificare i diritti di accesso ad un oggetto o non è necessario consultare una struttura dati centralizzata associata a tutti gli oggetti
- ma basta manipolare una struttura dati molto più snella, distribuita ed associata soltanto all'oggetto  $o$

Il principale svantaggio delle ACL è che non consente di enumerare in modo efficiente i diritti di accesso di un dato soggetto. Tale operazione deve essere espletata ogni qual volta un utente viene rimosso da un sistema. I diritti di accesso di un soggetto  $s$  possono ottenersi soltanto effettuando una scansione di tutte le liste di accesso (associate a tutti gli oggetti  $o$ ), e selezionando i diritti di accesso di  $s$  nelle liste in cui tale soggetto compare. Nel modello ACM, invece, ciò poteva banalmente ottenersi esaminando la riga della matrice relativa al soggetto  $s$ .

### 1.4.3 Controllod egli accessi basato su liste di capacità (Capabilities Access Control CAC)

Il modello basato sulle liste di capacità segue un approccio “subject-centered”, complementare (ortogonale) a quello del modello ACL, per offrire una buona scalabilità. Ad ogni soggetto  $s$  viene associata una lista, detta **C-list** di  $s$ , contenente soltanto gli oggetti per i quali  $s$  ha un qualche diritto di accesso. Per ciascun oggetto  $o$  della **C-list** di  $s$  viene specificato il tipo di azione che  $s$  può esercitare su  $o$ . Similmente al modello ACL, anche il modello CAC comporta un significativo risparmio di memoria rispetto al modello ACM nelle situazioni pratiche: ogni lista del modello CAC è ottenibile scandendo la relativa riga del modello ACM ignorando però le celle vuote.

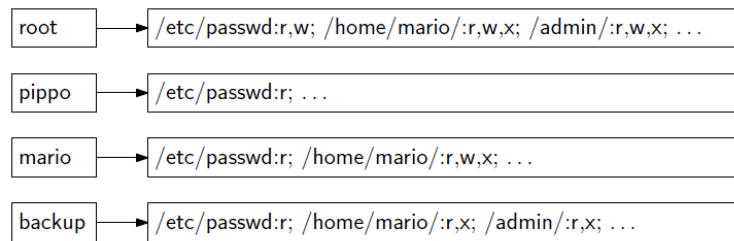


Figura 1.7: Esempio CAC

### Pro e Contro CAC

Rispetto al modello ACM, anche il modello CAC richiede una minor occupazione di memoria nella pratica. la memoria occupata complessivamente nel modello CAC,  $\sum_s size(L_s)$ , è proporzionale a  $C_{nv}(ACM)$ , cioè al numero di celle non vuote della ACM (vedi considerazioni su ACL). Facilita inoltre il compito dell'amministratore di sistema nell'analizzare e gestire i diritti di accesso di un dato soggetto. Inoltre, l'autorizzazione ad accedere ad un dato oggetto o da parte di un soggetto **s** richiede tempi ragionevolmente brevi qualora la **C-list** di **s** abbia una dimensione contenuta.

Il principale svantaggio del modello CAC è che le **C-list** non sono direttamente associate agli oggetti. Ciò comporta che:

- non è possibile implementarle in modo distribuito incorporandole nei metadati degli oggetti
- l'unico modo per determinare chi e come può accedere ad un dato oggetto o è effettuare una ricerca su tutte le C-list (di tutti i soggetti); nel modello ACM tale operazione richiede semplicemente di esaminare la colonna relativa ad o (problema ortogonale a quello delle ACL)

#### 1.4.4 Controllo degli accessi basato sui ruoli (Role-Based Access Control RBAC)

Per controllo degli accessi basato sui ruoli si intende che l'assegnazione dei diritti di accesso avviene in modo indiretto ed è funzione del ruolo attribuito ad un dato soggetto **s**. L'amministratore definisce i ruoli e specifica i diritti di accesso per tali ruoli, anziché quelli per i singoli soggetti (utenti). Ogni ruolo dovrebbe rappresentare una classe di soggetti (utenti) con la medesima mansione. I soggetti vanno assegnati ai vari ruoli coerentemente alle loro mansioni, e un soggetto può ricevere più ruoli dato che può ricoprire più mansioni. Definiti i ruoli, i diritti di accesso vanno assegnati secondo una logica ruolo-oggetto e NON soggetto-oggetto. I diritti di accesso di un dato soggetto sono l'unione dei diritti di accesso dei suoi ruoli. Pertanto:

- textbfil modello RBAC non 'è alternativo ai modelli ACM, ACL e CAC, ma si pone ad un livello di astrazione superiore: RBAC deve necessariamente sfruttare un modello per il controllo degli accessi, basato su **ACM**, **ACL** o **CAC**, ove i soggetti saranno però sostituiti dai ruoli.
- RBAC deve inoltre mantenere/gestire l'elenco dei ruoli associati ai vari soggetti

### Architettura RBAC

Il modello RBAC 'è realizzabile utilizzando un generico framework per la gestione del controllo degli accessi (ACM, ACL, CAC), ove i soggetti sono, come già detto, sostituiti con i ruoli, più un layer superiore che gestisce l'elenco dei ruoli associati ai vari soggetti e che traduce le richieste di accesso per un dato soggetto in quelle relative ai suoi ruoli.

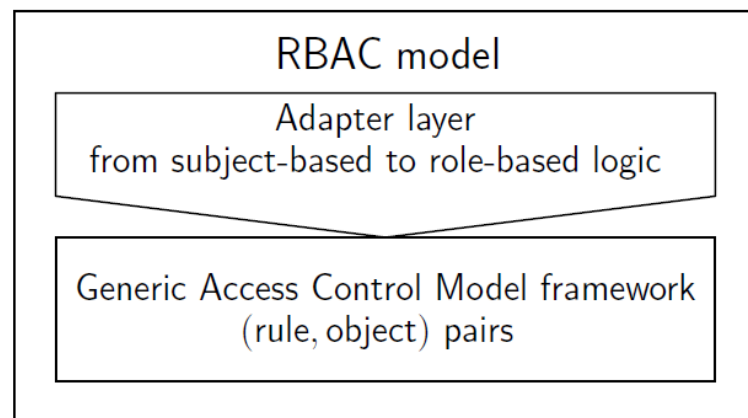


Figura 1.8: Architettura RBAC

### Gerarchia dei ruoli

Generalmente è conveniente organizzare i ruoli in una struttura gerarchica, così da riflettere l'organigramma (gerarchico) di una data organizzazione. I diritti di accesso vengono più agevolmente gestiti e assegnati ai vari ruoli sfruttando l'ereditarietà.

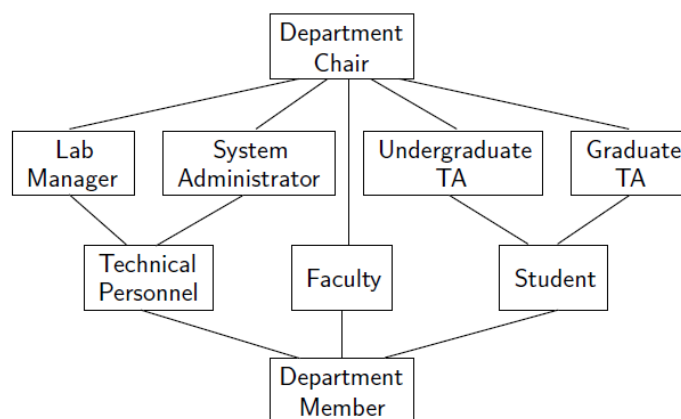


Figura 1.9: Architettura RBAC

### Pro e Contro RBAC

Indipendentemente dal framework di basso di livello utilizzato per il controllo degli accessi, i vantaggi nell'uso del modello RBAC sono:

- la riduzione drastica del numero totale di regole di accesso da gestire; nella pratica il numero dei ruoli è significativamente inferiore a quello dei soggetti, inoltre la loro organizzazione gerarchica ne semplifica ulteriormente la gestione.
- l'overhead per determinare se un dato soggetto ha un dato diritto è contenuto, è sufficiente consultare se almeno uno dei suoi ruoli ha tale diritto.

Lo svantaggio principale è che non viene implementato dagli attuali sistemi operativi!

## Capitolo 2

# Secret Key Cryptography

### 2.1 Introduzione

La crittografia a chiave segreta richiede l'uso di UNA sola chiave: dato un messaggio (il testo in chiaro) e la chiave, la cifratura produce dati non intellegibili (il testo cifrato). Il testo cifrato ha circa la stessa lunghezza di quello in chiaro e la decifratura è l'inverso della cifratura, ed usa la stessa chiave. La crittografia a chiave segreta è talvolta chiamata crittografia **convenzionale** o crittografia **simmetrica**.

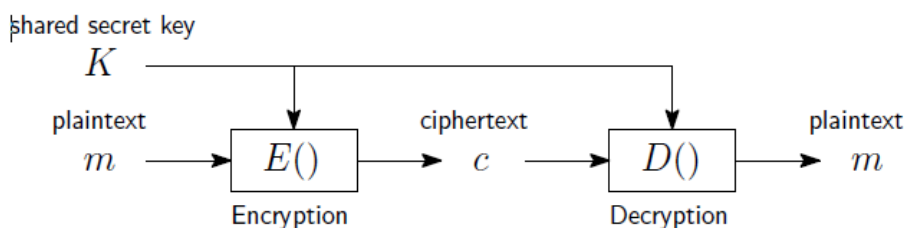


Figura 2.1: Schema a blocchi crittografia a chiave segreta

#### 2.1.1 Impieghi crittografia a chiave segreta

La crittografia a chiave segreta è alla base di molti meccanismi di sicurezza, i suoi principali impieghi sono:

- protezione della **confidenzialità** (l'uso classico di queste tecniche è rappresentato dalle **comunicazioni su un canale insicuro**, uno degli usi più moderni invece dalla **memorizzazione sicura su supporto insicuro**)
- protezione dell'**integrità**: tramite queste tecniche possono essere eseguiti test per rilevare eventuali modifiche non consentite.
- autenticazione: tramite l'implementazione di protocolli per verificare l'identità di persone e/o processi.

#### Comunicazioni su un canale insicuro

In molte circostanze, due entità devono comunicare attraverso un canale insicuro correndo il rischio di essere ascoltate da una terza parte. Questo contesto è molto comune: si pensi alle reti LAN, che trasmettono dati in broadcast. La crittografia a chiave segreta permette a due entità che condividono un segreto (la chiave) di comunicare attraverso un canale insicuro, ove non può

essere garantita l'assenza di intercettazioni/ascoltatori (eavesdropper), avendo la garanzia che il contenuto della comunicazione rimarrà confidenziale.

### Memorizzazione sicura

Si supponga di disporre di un supporto di memorizzazione non protetto (ad esempio accessibile a molti utenti). Se si desidera salvare i dati proteggendone la confidenzialità si può definire una chiave segreta, salvare i dati dopo averli crittografati con tale chiave e custodire la chiave segreta in un luogo protetto. Il rischio dell'uso di questa tecnica consiste nella possibilità di smarrimento della chiave. In tal caso i dati sarebbero irrevocabilmente persi.

### Autenticazione forte

Per **autenticazione forte (strong authentication)** si intende che si è in grado di provare la conoscenza di un segreto, che contraddistingue l'identità di una data entità, senza rivelarlo. L'autenticazione forte è ottenibile utilizzando la crittografia a chiave segreta, ed è particolarmente utile quando due processi devono comunicare su una rete insicura. A rigore il segreto che contraddistingue l'identità che si desidera autenticare dovrebbe essere noto solo a quest'ultima. Nella crittografia chiave segreta tale requisito non può essere soddisfatto. Il segreto in questione è una chiave crittografica che deve essere nota anche all'entità autenticante.

### Esempio

Si supponga che Alice e Bob condividano una chiave segreta  $K_{AB}$  e che vogliano autenticarsi reciprocamente, cioè ciascuno vuole accertarsi dell'identità dell'altro.

**ipotesi:**  $K_{AB}$  è nota solo ad Alice e Bob. Alice deve dimostrare a Bob di conoscere  $K_{AB}$  senza rivelarla e viceversa.

**Strategia a sfida e risposta:** ciascuno dimostra di conoscere  $K_{AB}$  rispondendo ad una sfida posta dall'altro. La **sfida** è un numero/stringa random  $r$  non prevedibile e sempre diversa. La **risposta** alla sfida è la sfida stessa cifrata  $E(K_{AB}, R)$ . In Figura 2.2 è riportato un possibile schema di autenticazione a sfida e risposta (challenge-response) a chiave segreta. La procedura segue i seguenti passi:

- Alice genera un numero random  $r_A$  (la sfida) e la invia al presunto Bob
- il presunto Bob critta la sfida con la sua chiave segreta  $K'_{AB}$  e restituisce ad Alice la risposta  $E(K'_{AB}, r_A)$
- Alice riceve la risposta del presunto Bob e la decritta con la chiave  $K_{AB}$ , cioè calcola  $D(K_{AB}, E(K'_{AB}, r_A))$ . Se ottiene  $r_A$ , allora il presunto Bob è realmente Bob poiché con elevatissima probabilità, se  $D(K_{AB}, E(K'_{AB}, r_A)) = r_A$ , allora  $K'_{AB} = K_{AB}$ . In caso negativo deduce invece che il presunto Bob è un impostore. In modo analogo Bob verifica l'identità di Alice.

La sicurezza del precedente protocollo si fonda sulle seguenti condizioni che non devono venire meno:

- solo e soltanto Alice e Bob devono conoscere la chiave segreta  $K_{AB}$
- le sfide generate devono essere **randomiche**, e di conseguenza non prevedibili, e **non ripetibili**, cioè la probabilità che due sfide si ripetano deve tendere a zero. L'attaccante potrebbe infatti collezionare molte coppie testo in chiaro/testo cifrato.
- è importante quindi che il numero di bit di una sfida sia superiore ad una data soglia (almeno 64 bit)

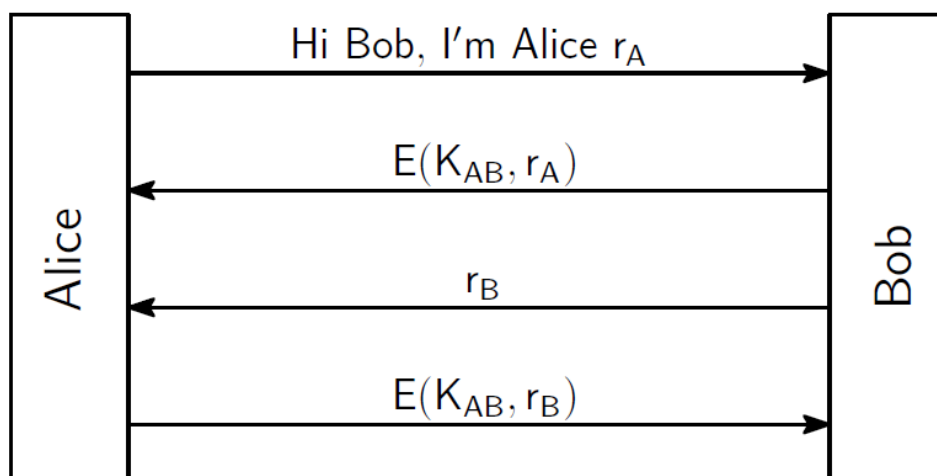


Figura 2.2: Schema a blocchi crittografia a chiave segreta

### Controllo di integrità

La verifica dell'integrità di un messaggio inviato o di un file è un problema ricorrente in telecomunicazioni e in informatica. Per rilevare eventuali modifiche accidentali si fa uso generalmente di codici (somme) di controllo, detti anche **checksum**. Un **checksum** associa ad un qualsiasi messaggio  $\mathbf{m} \in \{0, 1\}^*$  un codice di lunghezza prefissato di  $b$  bit (generalmente  $b = 32, 64, 128$  bit):  $ck(\mathbf{m}) \in \{0, 1\}^b$ . Un buon **checksum** dovrebbe variare in modo significativo anche a fronte di minime variazioni dell'input.

La sorgente del messaggio  $m_s$  rende pubblico/invia il corrispondente checksum  $ck(m_s)$ . Chi riceve il messaggio  $m_r$  calcola il checksum e verifica se vale l'uguaglianza  $ck(m_s) = ck(m_r)$ . In caso affermativo, conclude che  $m_s = m_r$ . Si noti tuttavia che, seppur improbabile, è possibile ottenere dei falsi positivi, cioè  $ck(m_s) = ck(m_r)$  anche se non è vero.

### Checksum segreti e non segreti

I codici di controllo servono per proteggere l'hardware da difetti e da inevitabili errori/guasti. Esistono codici di controllo molto sofisticati come i **CRC (Cyclic Redundancy Check)** per i quali la probabilità di falsi positivi è estremamente ridotta. Esistono anche i codici **FEC (Forward Error Correction)** che permettono di correggere eventuali errori oltre che a rilevarli (aggiungendo ulteriore ridondanza). Tuttavia entrambe queste tecniche **non** sono utilizzabili per la protezione contro attacchi intelligenti. Essendo pubblici, infatti, un avversario intelligente che vuole cambiare un messaggio potrebbe modificare anche il codice di controllo in maniera coerente.

Per la protezione contro modifiche maliziose ad un messaggio, è richiesto un codice di controllo (checksum) segreto. Se l'algoritmo non è noto, nessuno può calcolare il checksum corretto per il messaggio modificato. Chiaramente, come nel caso degli algoritmi di cifratura, anziché un algoritmo segreto conviene avere un algoritmo noto a tutti che richiede la conoscenza di una chiave segreta per il calcolo di un codice di controllo (Vedi pagina 9, principio **Open Structure**).

In ciò consiste appunto un checksum cifrato, detto anche **MIC (Message Integrity Code)**. Il funzionamento del MIC è il seguente:

- l'algoritmo produce un codice di autenticazione di lunghezza fissa  $MIC(K, m)$ , denominato anche **MAC (Message Authentication Code)**
- il codice MIC  $MIC(K, m)$  viene trasmesso insieme al messaggio  $m$  stesso

- formalmente l'input è una coppia  $(K, m) \in \{0, 1\}^k \times \{0, 1\}^*$ , dove  $k$  denota il numero di bit della chiave segreta  $K$ , mentre l'output è sempre una stringa binaria di lunghezza prefissata, cioè  $MIC(K, m) \in \{0, 1\}^b$

### 2.1.2 Cifrari a blocchi e cifrari a flusso

Un **cifrario a blocchi** elabora un blocco di elementi in ingresso per volta, producendo un blocco di uscita per ciascun blocco di ingresso. Questa metodologia implica quindi che:

- il testo in chiaro deve essere preliminarmente suddiviso in blocchi
- il testo cifrato si ottiene combinando i vari blocchi cifrati

DES, IDEA e AES sono esempi di cifrari a blocchi simmetrici. Un **cifrario a flusso**, invece, elabora continuamente gli elementi in ingresso, producendo in uscita un "flusso" di elementi cifrati. Gli elementi cifrati vengono prodotti singolarmente, uno alla volta, man mano che la cifratura procede.

## 2.2 Cifratura a blocchi

### 2.2.1 Introduzione e concetti generali

L'algoritmo di cifratura converte un blocco di testo in chiaro in un blocco di testo cifrato. La chiave  $K$  non deve essere troppo corta (e.g. se  $K$  ha lunghezza 4 bit, sono sufficienti  $2^4 = 16$  tentativi per individuarla). Analogamente la lunghezza (fissata) di un blocco non deve essere troppo piccola (e.g. se un blocco ha lunghezza 8 bit, ottenendo delle coppie plaintext - ciphertext si potrebbe costruire una tabella di  $2^8 = 256$  coppie utilizzabile per la decifrazione).

D'altra parte, avere blocchi esageratamente lunghi oltre a non essere necessario dal punto di vista della sicurezza, comporta una gestione più complicata e può degradare le prestazioni. **64 bit è una lunghezza ragionevole per un blocco:**

- è improbabile ottenere ordine di  $2^{64}$  coppie  $\langle \text{plaintext}, \text{ciphertext} \rangle$  per costruire una tabella di decifrazione, e
- anche se fosse possibile, la sua memorizzazione richiederebbe uno spazio enorme ( $2^{64}$  record da 64 bit),
- come pure l'ordinamento per consentire ricerche efficienti

Il modo più generale per cifrare un blocco da 64 bit è definire una **biiezione**  $\gamma : \{0, 1\}^{64} \rightarrow \{0, 1\}^{64}$ . Tuttavia, memorizzare la definizione della *biiezione* in una struttura dati è impraticabile: sarebbero richiesti  $2^{64} \times 64 = 2^{70}$  bit. Ad essere precisi ce ne vogliono un po' di meno, trattandosi di un **biiezione**, comunque almeno  $2^{69}$  bit sono richiesti (**perché?!?!).** Inoltre, così facendo la chiave è incorporata nella biiezione: per renderla parametrica rispetto alla chiave è necessario memorizzare una biiezione per ogni possibile chiave.

I sistemi di crittografia a chiave segreta sono concepiti per usare una chiave ragionevolmente lunga (ad esempio 64 bit) e generare una **biiezione** che appare, a chi non conosce la chiave, completamente random. Se la biiezione fosse realmente random due input  $i$  e  $i'$  nei quali cambia un solo bit (uno qualunque) sarebbero **statisticamente indipendenti**: non può succedere, ad esempio, che il terzo bit dell'output cambia **sempre** quando il dodicesimo bit dell'input cambia. Gli algoritmi crittografici sono pensati per **diffondere/spargere** in tutti i bit dell'output il valore di ogni bit dell'input: si cerca di far sì che ogni bit dell'output dipenda allo stesso modo da tutti i bit dell'input.



### 2.2.2 Sostituzione e Permutazione

Sostituzioni e permutazioni sono due trasformazioni base applicabili ad un blocco di dati.

Si assuma di dover cifrare un blocco di  $k$  bit. Una **sostituzione** specifica, per ciascuno dei  $2^k$  possibili valori dell'input, i  $k$  bit dell'output. Per specificare una sostituzione "**completamente random**" sono necessari circa  $k2^k$  bit. E' quindi impraticabile implementare una sostituzione per blocchi di 64 bit, mentre è fattibile per blocchi di lunghezza di 8 bit. Esempio di crittografia per sostituzione è il **Cifrario di Cesare**.

Una **permutazione** specifica, per ciascuna delle  $k$  posizioni dei bit in input, la posizione del corrispondente bit nell'output. Per specificare una permutazione "**completamente random**" per un blocco di lunghezza  $k$  bit sono necessari  $k \log_2 k$  bit. Infatti per ciascuno dei  $k$  bit va specificata la sua posizione nell'output; ogni posizione richiede  $\log_2 k$ . Ad esempio: essendo  $2^6 = 64$ , sono necessari  $6 = \log_2 64$  bit per specificare la nuova posizione che l' $i$ -esimo bit in input avrà in output.

Si noti che una **permutazione** è un caso particolare di **sostituzione** in cui ogni bit dell'output ottiene il suo valore da esattamente un bit dell'input.

### 2.2.3 Cifrario a blocchi – schema generale

Un algoritmo di cifratura a chiave segreta può funzionare come segue:

- scompone il blocco in input in pezzi più piccoli (e.g. blocchi da 8 bit)
- applica una sostituzione (tramite una **rete combinatoria**) a ciascun pezzo da 8 bit (la sostituzione dipenderà dal valore della chiave)
- gli output delle sostituzioni vengono riuniti in un unico blocco (64 bit)
- tale blocco viene permutato in un permutatore a 64 bit (che ha il compito di diffondere le modifiche eseguite nelle sostituzioni)
- il processo viene ripetuto un certo numero di volte riportando l'output in ingresso

### 2.2.4 Cifrario a blocchi – esempio

Ogni attraversamento del cifrario viene detto **round**. In riferimento alla Figura 2.3 si fanno le seguenti considerazioni. Con un solo round, un bit  $b_x$  di input può influenzare soltanto 8 bit  $b_{x1}, b_{x2}, \dots, b_{x8}$  dell'output, poiché  $b_x$  ha attraversato soltanto un blocco di sostituzione. In generale i bit  $b_{x1}, b_{x2}, \dots, b_{x8}$  non sono consecutivi essendo stati mescolati nel permutatore. Alla fine del secondo round, assumendo che i bit  $b_{x1}, b_{x2}, \dots, b_{x8}$  siano smistati in blocchi di sostituzione distinti, il bit  $b_x$  iniziale influenza tutti i bit in output.

## 2.3 Data Encryption Standard - DES

DES fu pubblicato nel 1977 dal **National Bureau of Standards**, ora rinominato **National Institute of Standards and Technology (NIST)**, per usi commerciali e "altre" applicazioni del governo statunitense. Progettato da IBM, si basa sul precedente cifrario *Lucifer* ed è frutto della collaborazione con consulenti della NSA. DES usa una chiave di 56 bit, e mappa un blocco di input da 64 bit in un blocco di output da 64 bit (l'algoritmo è quindi abbastanza rigido, al contrario di altri cifrari a blocchi). La **chiave** è in realtà costituita da una sequenza di 64 bit, ma un bit in ogni ottetto (il blocco da 64 bit è formato da 8 sequenze di 8 bit dette ottetti) è usato come **odd parity** su ciascun ottetto. Di fatto, soltanto 7 bit in ogni ottetto sono quindi veramente significativi come chiave.

## Block Ciphers

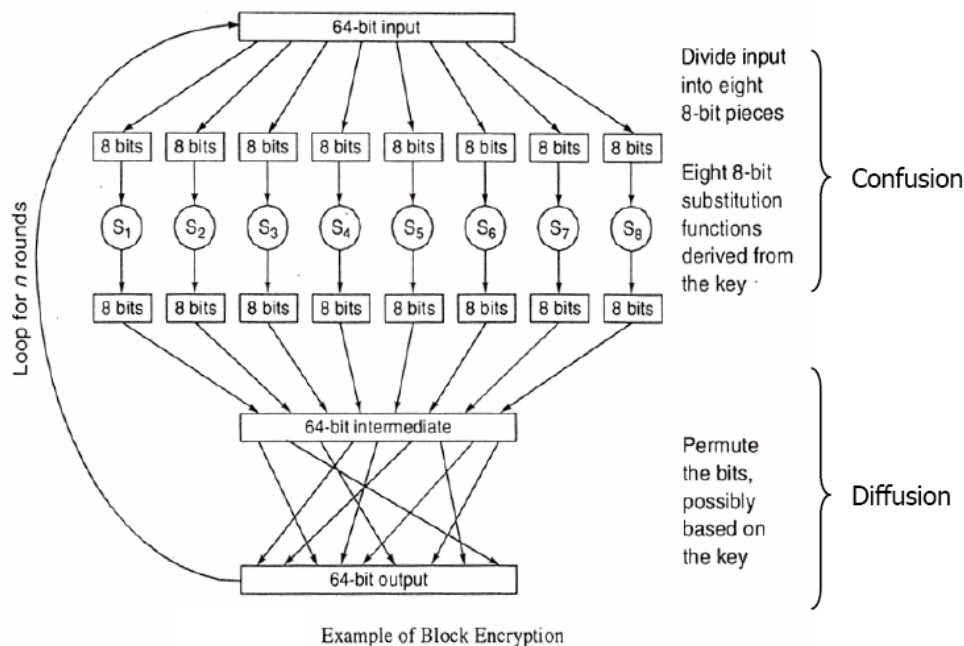


Figura 2.3: Schema a blocchi crittografia a chiave segreta

DES è efficiente se realizzato in hardware, ma relativamente lento se implementato in software. Sebbene l'essere difficilmente implementabile come software non fosse un requisito specificato nel progetto molti sostengono che in realtà questa mancanza fosse voluta, forse per limitarne l'uso ad organizzazioni in grado di realizzare sistemi hardware, o forse perché rese più facile controllare l'accesso alla tecnologia. Ad ogni modo, l'aumento delle capacità di calcolo delle CPU rese possibile realizzare una versione software di DES. Una 500-MIPS (Million Instruction Per Second) CPU può infatti cifrare ad un tasso di circa 30 KB/s e forse più, a seconda dei dettagli architetturali della CPU e dell'intelligenza dell'implementazione. Un processore Intel Core i7 Extreme Edition i980EE ha una capacità di calcolo di circa 150 MIPS, quindi può cifrare ad un tasso di circa 9 KB/s (per cifrare 1 MB impiega circa 110 secondi). L'implementazione software è pertanto attualmente adeguata a molte applicazioni.

### 2.3.1 Perché chiavi da 56 bit?

La scelta di una chiave da 56 bit causò molte controversie. Prima che DES fu adottato, le persone al di fuori della *intelligence community* lamentavano che 56 bit non offrivano una sicurezza adeguata. Perché solo 56 dei 64 bit di una chiave DES sono effettivamente usati nell'algoritmo? Lo svantaggio di usare 8 bit della chiave per un controllo di parità è che ciò rende DES molto meno sicuro (256 volte meno sicuro contro una ricerca esaustiva). Ma qual è il vantaggio di usare 8 bit per un controllo di parità? Una possibile risposta è che permette di verificare che la chiave non sia corrotta. Tuttavia questa spiegazione non regge. Se si considerassero infatti 64 bit a caso invece della chiave, c'è una probabilità su 256 che il controllo di parità dia esito positivo. La probabilità che la chiave sia comunque errata (nonostante il controllo di parità dia esito positivo) è troppo alta. Inoltre avere una chiave corrotta non comporta un problema di sicurezza, semplicemente la cifratura/decifratura non viene eseguita correttamente. Chiaramente è anche ridicolo sostenere che la scelta di 56 bit sia stata fatta per risparmiare memoria.

La risposta ormai condivisa è che il governo statunitense abbia deliberatamente indebolito la sicurezza di DES di una quantità appena sufficiente da consentire alla NSA di violarlo.

### 2.3.2 Violabilità e sicurezza di DES

Gli avanzamenti tecnologici dell'industria dei semiconduttori hanno reso ancora più critico il problema della lunghezza della chiave di DES. la velocità dei chip e un po' di furbizia permettono di violare (individuare) le chiavi DES con approcci a forza bruta in tempi ragionevoli. Il rapporto prestazioni/prezzo dell'hardware cresce del 40% per anno. La lunghezza delle chiavi dovrebbe aumentare di 1 bit ogni 2 anni. Assumendo che 56 bit erano appena sufficienti nel 1979 (quando DES fu standardizzato), 64 bit erano adeguati nel 1995, e 128 bit dovrebbero essere sufficienti fino al 2123.

Ragioniamo ora sulla sicurezza di DES. Se si dispone di un singolo blocco  $\langle \textit{plaintext}, \textit{ciphertext} \rangle$  quanto è difficile trovare la chiave? Un approccio a forza bruta dovrebbe provare ordine di  $2^{56} \approx 10^{17}$  chiavi. Se ogni tentativo richiede una singola istruzione sono necessarie ordine di 1000 MIPS-year istruzioni.

- 1 MIPS = 1 Milione di Istruzioni Per Secondo
- 1 MIPS-year = numero di istruzioni eseguite in un anno ad un tasso pari a 1 MIPS
- 1 MIPS-year = 1 MIPS  $\times$  (365  $\times$  86400) secondi in un anno =  $3,1536 \times 10^{13}$  istruzioni
- $2^{56} \approx 10^{17} \approx 10^3$  MIPS-year

Questo vale tuttavia **SOLO** per effettuare una ricerca esaustiva. Dopo di che entra in gioco il fatto che io sappia riconoscere o meno il testo in chiaro.

### 2.3.3 Violabilità DES - esempio

Anche nell'ipotesi più scomoda per l'avversario di disporre solo di testo cifrato (in ragionevole quantità), un attacco a forza bruta è ancora possibile. Se ad esempio l'avversario sa soltanto che il testo in chiaro è ASCII a 7 bit ogni volta che prova una chiave deve verificare se sono nulli tutti i bit nelle posizioni 8, 16, 24, ...,  $n \times 8$ , .... Per ogni blocco di 64 bit, vanno esaminati solo 8 bit; i bit in posizione 8, 16, 24, 32, 40, 48, 56, 64. Se almeno uno di questi bit vale 1 la chiave è sicuramente errata. in caso contrario nulla si può dire; **la probabilità di errore è pertanto 1 su 256 ossia la probabilità che tutti questi bit valgano 0**. Se l'avversario esamina diversi blocchi, ad esempio 10, e verifica che si tratta sempre di ASCII a 7 bit la probabilità che la chiave scelta sia errata si riduce a 1 su 2560. Si noti che gli attuali chip commerciali che implementano DES non si prestano a ricerche esaustive della chiave: sono pensati per cifrare molti dati con una stessa chiave. Infatti il caricamento di una chiave è un'operazione lenta se confrontata con la velocità con la quale viene eseguita la cifratura dei dati. Tuttavia è sempre possibile costruire un chip ottimizzato ad eseguire ricerche esaustive della chiave.

### 2.3.4 Violabilità DES - cifratura multipla

Per ovviare a tali problemi di sicurezza è possibile cifrare più volte e con diverse chiavi lo stesso blocco di dati. Si parla di **cifratura multipla (multiple encryption)**. Si ritiene che una cifratura con un triplo DES sia  $2^{56}$  volte più difficile da violare.

### 2.3.5 DES - Struttura base

La struttura di base dell'algoritmo DES è descritta in Figura 2.4. In estrema sintesi:

- L'input di 64 bit è sottoposto ad una permutazione iniziale;
- La chiave da 56 bit viene usata per generare 16 per-round chiavi da 48 bit; una chiave per ciascuno dei 16 round, prendendo 48 differenti sottoinsiemi dei 56 bit della chiave

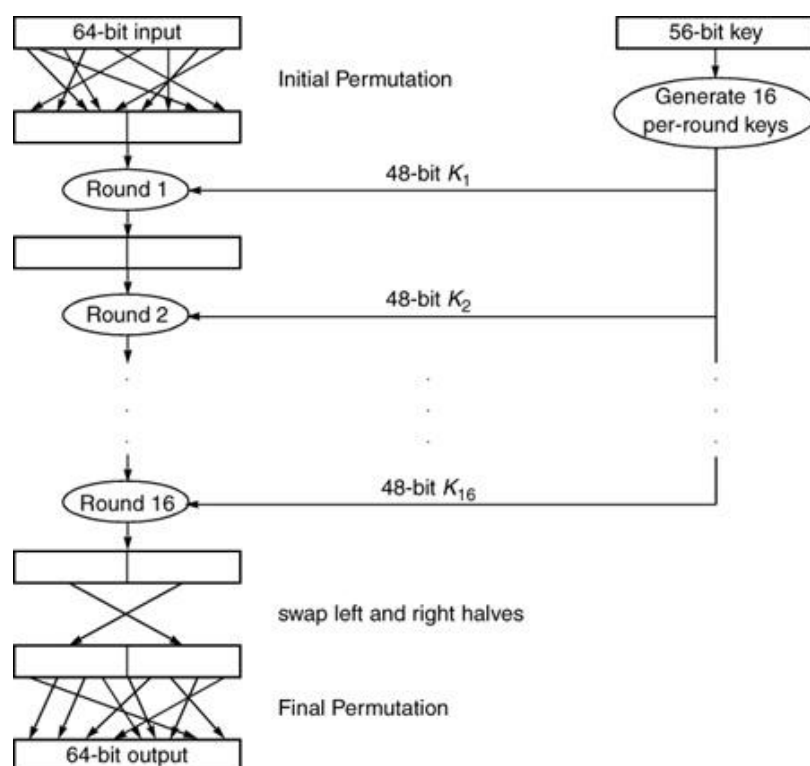


Figura 2.4: Schema a blocchi DES

- Ogni round riceve in input l'output di 64 bit del round precedente e la chiave da 48 bit di quel round
- Ogni round restituisce un output di 64 bit
- Dopo il 16-esimo round, le due metà dell'output di 64 bit vengono scambiate e il risultato viene sottoposto ad un'altra permutazione (inversa a quella iniziale)
- La decifratura consiste semplicemente nell'eseguire la cifratura DES all'indietro
- Per decifrare un blocco è necessario applicare la permutazione iniziale (ciò annulla l'effetto della permutazione finale), generare le 16 chiavi di round, che andranno usate in ordine inverso (prima  $K_{16}$ , l'ultima chiave generata), seguire 16 round esattamente come nella cifratura, scambiare le due metà dell'output e sottoporle a un'altra permutazione (che annulla l'effetto della permutazione iniziale)

Per descrivere DES è quindi sufficiente discutere le permutazioni iniziale e finale, come le chiavi di round sono generate, e cosa succede durante un round.

### 2.3.6 DES - Permutazioni dei dati

L'operazione di permutazione è molto importante in quanto diffonde la dipendenza dei bit in/out. Nel caso di DES però le permutazioni finale e iniziale non hanno effetto. Dimostriamo tale affermazione.

Supponiamo di non averle. Se assumiamo per assurdo che il cifrario così ottenuto sia facile da violare, vogliamo dimostrare che anche DES è facile da violare. Chiamiamo il cifrario senza permutazione EDS. Se posso violare EDS (disponendo, ad esempio, di una coppia  $\langle \text{plaintext}, \text{ciphertext} \rangle$ ), basta permutare ciò che ottengo e violo DES. Infatti, sia  $\langle m, c \rangle$  una coppia  $\langle \text{plaintext}, \text{ciphertext} \rangle$  di DES. Si consideri allora la coppia  $\langle m', c' \rangle$ , dove  $m'$  e  $c'$  sono ottenuti applicando la permutazione iniziale ad  $m$  e  $c$ . Allora, la chiave  $K_{EDS}$  che si ottiene

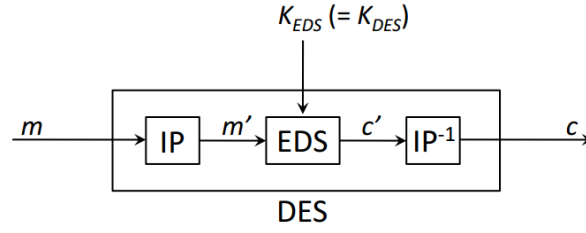


Figura 2.5: Inutilità delle permutazioni iniziale e finale

violando EDS per la coppia  $\langle m', c' \rangle$  coincide con la chiave  $K_{DES}$  di DES per la coppia  $\langle m, c \rangle$  (vedi Figura 2.5). L'ipotesi è che tali permutazioni siano state introdotte per rendere più complicata una possibile implementazione software. Come sono state definite quindi le permutazioni

Initial Permutation (IP)								Final Permutation (IP <sup>-1</sup> )							
58	50	42	34	26	18	10	2	40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	49	17	57	25

Figura 2.6: Tabella permutazioni DES

iniziale e finale? E' di fatto una permutazione regolare, come è mostrato in Figura 2.6. Le tabelle vanno interpretate nel seguente modo: i numeri, da 1 a 64, riportati in tabella rappresentano le posizioni dei bit in input alla permutazione, mentre l'ordine (per righe da sx verso dx) dei numeri nella tabella rappresenta la corrispondente posizione dei bit in output. Ad esempio, la permutazione iniziale sposta il 58-esimo bit in input nel primo bit in output, e il 50-esimo bit in input nel secondo bit in output. Non si tratta di permutazioni generate in modo random, in quanto presenta delle evidenti regolarità, come è evidenziato in Figura 2.7.

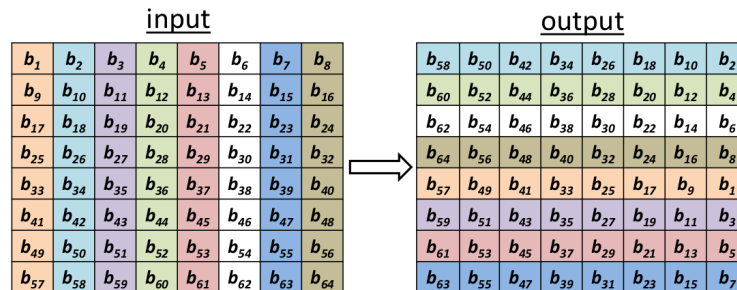


Figura 2.7: Regolarità tabella permutazioni DES

### 2.3.7 DES - Generazione chiavi di round

DES genera sedici chiavi di round da 48 bit a partire dalla chiave principale  $K$  di 64 bit nominali, di cui solo 56 effettivi. I bit di parità di  $K$  non vengono infatti considerati. Denoteremo con  $K_1, K_2, \dots, K_{16}$  le sedici chiavi di round. Il procedimento è il seguente:

- viene prima effettuata una permutazione iniziale sui 56 bit effettivi di  $K$
- i 56 bit in output vengono divisi in due metà  $C_0$  e  $D_0$
- Le sedici chiavi vengono generate in sedici round, i.e. nell' $i$ -esimo round viene generata la chiave di round  $K_i$

#### Permutazione iniziale

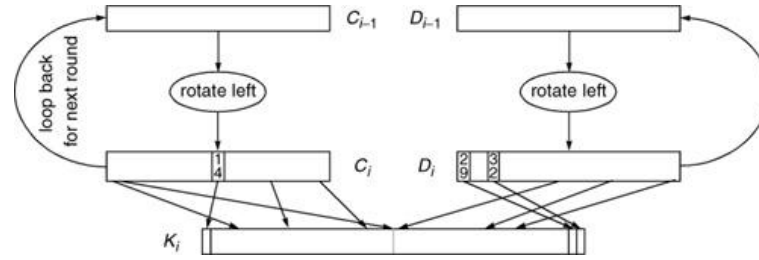
$C_0$							$D_0$						
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

Figura 2.8: Permutazione iniziale della chiave

input							output						
$b_1$	$b_2$	$b_3$	$b_4$	$b_5$	$b_6$	$b_7$	$b_{57}$	$b_{49}$	$b_{41}$	$b_{33}$	$b_{25}$	$b_{17}$	$b_9$
$b_9$	$b_{10}$	$b_{11}$	$b_{12}$	$b_{13}$	$b_{14}$	$b_{15}$	$b_1$	$b_{58}$	$b_{50}$	$b_{42}$	$b_{34}$	$b_{26}$	$b_{18}$
$b_{17}$	$b_{18}$	$b_{19}$	$b_{20}$	$b_{21}$	$b_{22}$	$b_{23}$	$b_{10}$	$b_2$	$b_{59}$	$b_{51}$	$b_{43}$	$b_{35}$	$b_{27}$
$b_{25}$	$b_{26}$	$b_{27}$	$b_{28}$	$b_{29}$	$b_{30}$	$b_{31}$	$b_{19}$	$b_{11}$	$b_3$	$b_{60}$	$b_{52}$	$b_{44}$	$b_{36}$
$b_{33}$	$b_{34}$	$b_{35}$	$b_{36}$	$b_{37}$	$b_{38}$	$b_{39}$	$b_{63}$	$b_{55}$	$b_{47}$	$b_{39}$	$b_{31}$	$b_{23}$	$b_{15}$
$b_{41}$	$b_{42}$	$b_{43}$	$b_{44}$	$b_{45}$	$b_{46}$	$b_{47}$	$b_7$	$b_{62}$	$b_{54}$	$b_{46}$	$b_{38}$	$b_{30}$	$b_{22}$
$b_{49}$	$b_{50}$	$b_{51}$	$b_{52}$	$b_{53}$	$b_{54}$	$b_{55}$	$b_{14}$	$b_6$	$b_{61}$	$b_{53}$	$b_{45}$	$b_{37}$	$b_{29}$
$b_{57}$	$b_{58}$	$b_{59}$	$b_{60}$	$b_{61}$	$b_{62}$	$b_{63}$	$b_{21}$	$b_{13}$	$b_5$	$b_{28}$	$b_{20}$	$b_{12}$	$b_4$

Figura 2.9: Regolarità tabella permutazioni delle chiavi DES

La struttura della permutazione iniziale della chiave è illustrata in Figura 2.6. Il valore numerico di un elemento della tabella rappresenta la posizione del bit in input, mentre l'ordine nella tabella rappresenta la posizione del bit in output (come per le permutazioni dei dati). Anche in questo caso non è random, in quanto presenta delle evidenti regolarità, come è evidenziato in Figura 2.9. Come nel caso delle permutazioni iniziale e finale dei dati, non apportano alcun miglioramento alla sicurezza.

Generazione  $K_i$  nell' $i$ -esimo roundFigura 2.10: generazione di  $K_i$ : round  $i$ 

Trattiamo ora la generazione della chiave  $K_i$  che avviene nell' $i$ -esimo round. La procedura avviene seguendo questi passi (come mostrato in Figura 2.10):

- i bit delle due metà  $C_{i-1}$  e  $D_{i-1}$  della  $(i-1)$ -esima chiave  $K_{i-1}$  vengono ruotati (traslazione ciclica) a sinistra. L'entità della traslazione dipende dal round: nei round 1, 2, 9 e 16 si ha una rotazione a sinistra di un solo bit (i.e. il primo bit diventa l'ultimo bit a destra), mentre negli altri round si ha una rotazione a sinistra di due bit.
- la permutazione di  $C_i$  che produce la metà sinistra di  $K_i$  è illustrata sotto. Si noti che i bit in posizione 9, 18, 22, e 25 sono scartati.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2

- la permutazione di  $D_{i-1}$  ruotato, cioè di  $D_i$ , che produce la metà destra di  $K_i$  è illustrata sotto. Si noti che i bit in posizione 35, 38, 43, e 54 sono scartati; rimangono così 24 bit anziché 28.

41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

## 2.3.8 Un round di DES

La struttura di un round di des è illustrata in Figura 2.11). I 64 bit in input sono divisi in due metà da 32 bit:  $L_n$ , la metà sinistra dopo l' $(n-1)$ -esimo round, e  $R_n$ , la metà destra dopo l' $(n-1)$ -esimo round. L'output di 64 bit del round si ottiene concatenando le due metà:  $L_{n+1}$ , la metà sinistra dopo l' $n$ -esimo round, e  $R_{n+1}$ , la metà destra dopo l' $n$ -esimo round.  $L_{n+1}$  è semplicemente  $R_n$ , mentre  $R_{n+1}$  è ottenuto come segue:

- $R_n$  e  $K_n$  sono posti in input alla mangler function; la mangler function viene anche detta funzione di Feistel
- l'output della mangler function,  $mangler(R_n, K_n)$ , è una quantità di 32 bit; si noti che  $R_n, K_n$  sono composti da 32 e 48 bit rispettivamente
- l'output  $mangler(R_n, K_n)$  viene poi sommato (XOR) con  $L_n$
- il risultato ottenuto è  $R_{n+1} = mangler(R_n, K_n) \oplus L_n$

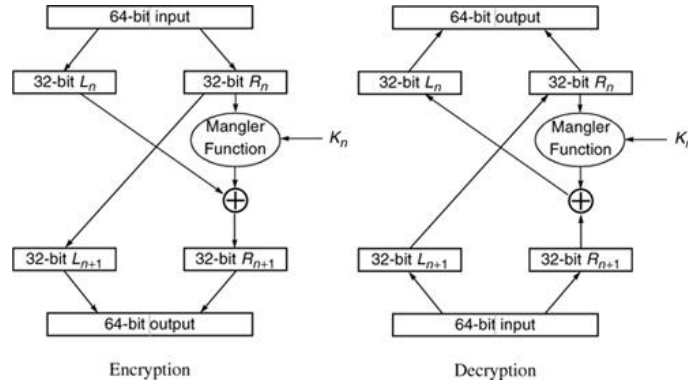


Figura 2.11: Struttura di un round di DES

Si noti che ogni round di DES è facilmente invertibile: noti  $L_{n+1}$ ,  $R_{n+1}$  e  $k_n$  è facile ottenere  $L_n$  e  $R_n$ . Infatti  $R_n = L_{n+1}$  e, poiché  $R_{n+1} = \text{mangler}(R_n, K_n) \oplus L_n$ , risulta  $R_{n+1} \oplus \text{mangler}(R_n, K_n) = L_n$  (in virtù della proprietà dello XOR secondo cui  $x \oplus y \oplus y = x$ ). La mangler function non è quindi mai utilizzata in senso inverso. DES è elegantemente progettato in modo da essere facilmente invertibile senza richiedere l'invertibilità della mangler function. Esaminando attentamente la Figura 2.11), si evince che la decifratura è di fatto identica alla cifratura, tranne per il fatto che le due metà da 32 bit sono invertite. In altre parole, fornendo  $R_{n+1} \mid L_{n+1}$  in input al round n si ottiene  $R_n \mid L_n$  in uscita.

### 2.3.9 Mangler Function

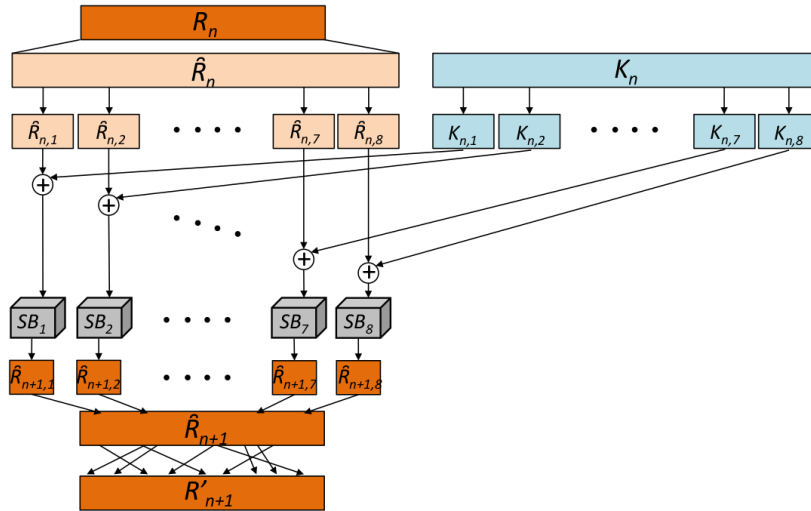


Figura 2.12: Mangler function

La mangler function prende in input i 32 bit di  $R_n$ , o  $R$  per semplificare, e i 48 bit della chiave  $K_n$ , o  $K$  per semplificare. Produce un output da 32 bit che sommato (XOR) con  $L_n$  permette di ottenere  $R_{n+1}$  (il prossimo  $R$ ).

La prima operazione è l'espansione di  $R$ , da 32 bit a 48 bit.  $R$  è scomposto in otto pezzi da 4 bit  $R = \{r_1, r_2, \dots, r_8\}$ . L' $i$ -esimo pezzo  $r_i$  viene espanso a 6 bit aggiungendo in testa e in coda rispettivamente l'ultimo bit di  $r_{i-1}$  e il primo bit di  $r_{i+1}$ .  $r_1$  e  $r_8$  sono considerati adiacenti, cioè  $r_0 = r_8$  e  $r_9 = r_1$ . (Fare riferimento alla Figura 2.13)).

la chiave  $K(K_n)$  viene scomposta in otto chunk (pezzi) da 6 bit. L' $i$ -esimo chunk di  $R(R_n)$  espanso viene sommato (XOR) all' $i$ -esimo chunk di  $K$ . L'output a 6 bit ottenuto viene sottoposto



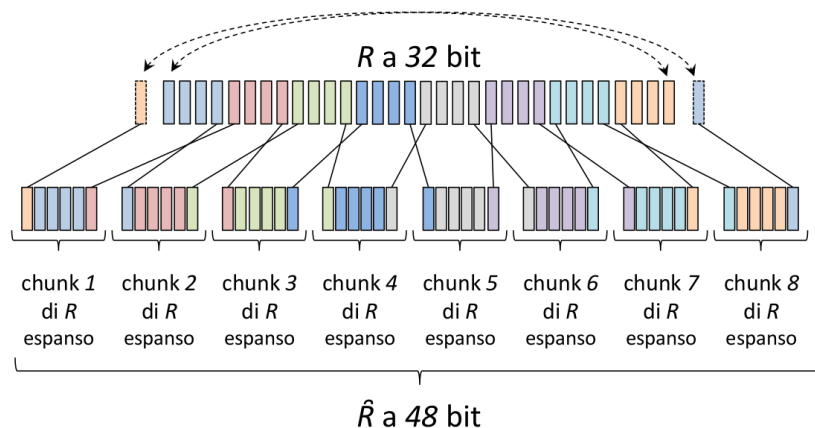


Figura 2.13: Mangler function - espansione

ad una sostituzione **S-box** che produce un output di 4 bit. Vi sono in tutto otto S-box distinte; l' $i$ -esima S-box elabora la somma dell' $i$ -esimo chunk di  $K$  e di  $R$ . Ogni S-box ha 64 possibili input e 16 possibili output. Ovviamente input diversi possono essere mappati nello stesso output (sto riducendo lo spazio). Le S-box sono definite in modo tale che esattamente quattro input distinti sono mappati in ciascun output possibile. Ogni S-box può riguardarsi come quattro S-box separate aventi 4 bit sia in input che in output: i quattro bit in input corrispondono ai bit interni (dal secondo al quinto) dell'input globale, e i due bit esterni (primo e sesto) dell'input globale servono a selezionare quale dei quattro output ottenuti rappresenta l'output globale. Infine gli

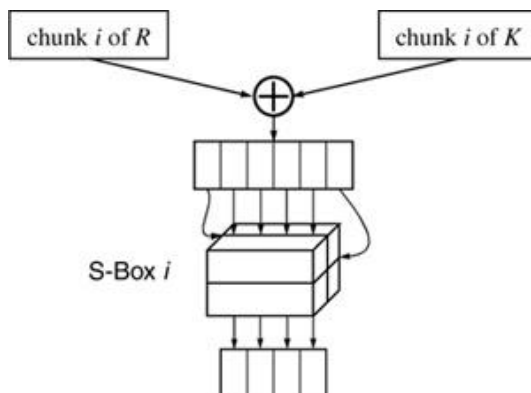


Figura 2.14: S-Box

otto output, da 4 bit, delle otto S-box sono riuniti in un unico output a 32 bit che viene sottoposto ad una permutazione. Tale permutazione aumenta il livello di sicurezza perché le sostituzioni fatte in ciascuna S-box in un round di DES vengono diffuse negli input di più S-box nel round seguente. Senza tale permutazione, un bit nella parte sinistra dell'input influenzerebbe principalmente alcuni bit della parte sinistra dell'output. Tale permutazione è mostrata in Figura 2.15).

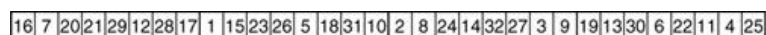


Figura 2.15: Permutazione output S-Box

## Capitolo 3

# Modes of Operation

### 3.1 Introduzione

Si illustrerà come usare gli algoritmi di crittografia a chiave segreta, DES, IDEA e AES, in applicazioni reali: è stato visto soltanto come usare tali algoritmi per cifrare blocchi di lunghezza prefissata (64 bit per DES e IDEA, 128 bit per AES), come si procede se è necessario cifrare dei messaggi di lunghezza arbitraria/diversa?

Si vedrà inoltre come si generano dei MAC (**M**essage **A**uthentication **C**ode) sfruttando la crittografia a chiave segreta.

### 3.2 Cifrare messaggi di grandi dimensioni

Come è possibile cifrare messaggi di dimensioni superiori a 64 bit?

Sono state proposte diverse **modalità operative dei cifrari a blocchi**, cioè ci si è interrogati su come utilizzare i cifrari a blocchi nel caso di messaggi di lunghezza maggiore di quella di un singolo blocco.

Le modalità più conosciute e che verranno descritte di seguito sono:

- **E**lectronic **C**ode **B**ook (ECB)
- **C**ipher **B**lock **C**haining (CBC)
- k-Bit **C**ipher **F**eed**B**ack Mode (CFB)
- k-Bit **O**utput **F**eed**B**ack Mode (OFB)
- **C**oun**T**e**R** Mode (CTR)

Si noti che nel seguito si farà riferimento a cifrari a blocchi con blocchi di 64 bit (tutte le considerazioni valgono anche nel caso di cifrari con blocchi di dimensione diversa da 64 bit).

#### 3.2.1 Electronic Code Book (ECB)

Questa modalità consiste nel fare la cosa più ovvia, ma corrisponde, in genere, alla soluzione peggiore, cioè:

- il messaggio viene decomposto in blocchi da 64 bit (inserendo eventualmente dei bit di padding nell'ultimo blocco al fine di riempirlo)
- ciascun blocco da 64 bit viene cifrato con la chiave segreta
- ciascun blocco cifrato viene decifrato

- il messaggio viene ricomposto a partire dai singoli blocchi decifrati

Come illustrato nella figure Figura 3.1 e Figura 3.2

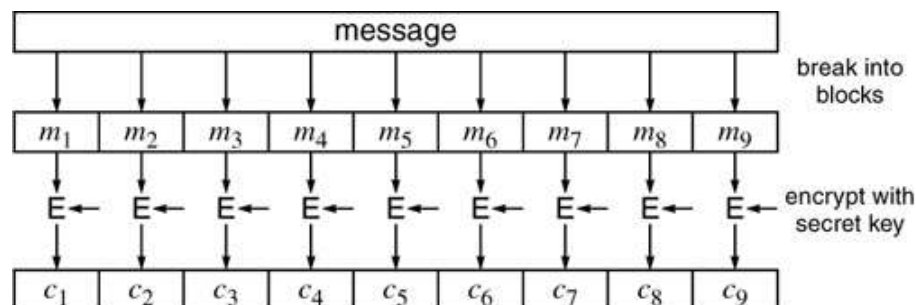


Figura 3.1: Schema di crittografia ECB

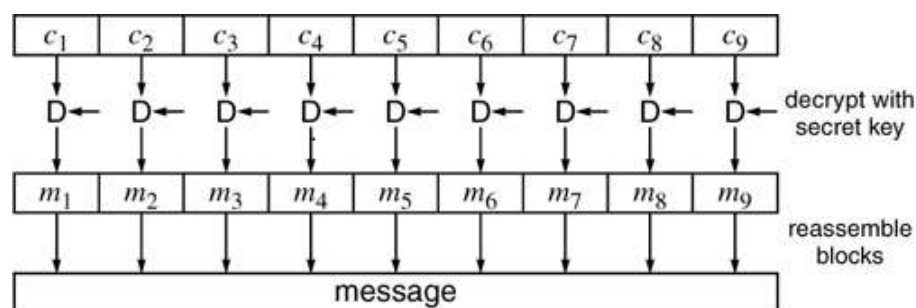


Figura 3.2: Schema di decrittografia ECB

### Problemi di sicurezza in ECB

La modalità operativa ECB introduce una serie di problemi non presenti nel cifrario a blocchi: se il messaggio contiene due blocchi di 64 bit identici, allora anche i corrispondenti blocchi cifrati saranno identici e ciò fornisce delle informazioni aggiuntive sul testo in chiaro che un ascoltatore può sfruttare. Si consideri ad esempio lo scenario della Figura 3.3: supponiamo che l'ascoltatore sappia che il testo in chiaro contiene l'elenco, ordinato alfabeticamente, degli impiegati e dei relativi salari inviato dall'amministrazione all'ufficio paghe, supponiamo inoltre che ogni riga del file sia lunga esattamente 64 byte (8 blocchi da 8 byte) e che i vari blocchi risultino suddivisi in modo tale che alcuni contengono la codifica della cifra decimale più significativa del campo salario (migliaia di dollari/euro). Comparando i testi cifrati, l'ascoltatore, oltre a dedurre quanti

Cognome	Nome	Posizione	Salario (€)
Bianchi	Walter	Impiegato	18.000,00
Neri	Marcello	Top Manager	70.000,00
Rossi	Carlo	Project Manager	40.000,00
Verdi	Dario	Tecnico	25.000,00
Viola	Saverio	Presidente	120.000,00

suddivisione in blocchi

Figura 3.3: File con i salari, oggetto di attacco

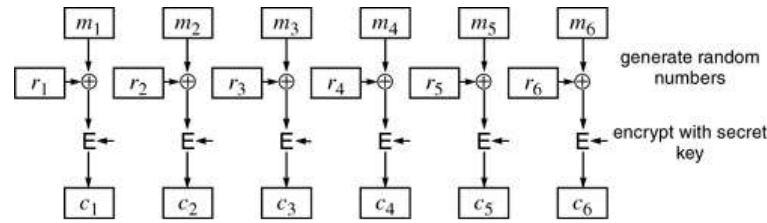


Figura 3.4: Randomized Electronic Code Book Encryption

dipendenti hanno lo stesso salario, può anche dedurre quanti dipendenti hanno uno stipendio nello stesso range (ordine di 10 euro/dollari); se ci sono complessivamente pochi range salariali, l'ascoltatore può dedurre a quale categoria di dipendente corrisponda un dato blocco cifrato; inoltre, se l'ascoltatore è un impiegato, può sostituire il blocco cifrato di un altro dipendente (un manager) al suo blocco cifrato (dedotto in base all'ordine e alla numerosità della sua classe salariale).

ECB quindi ha due serie debolezze, legate al fatto che qualcuno, analizzando diversi blocchi cifrati potrebbe:

- dedurre (inferire) informazioni sfruttando le ripetizioni di alcuni blocchi
- riarrangiare/modificare i blocchi cifrati a proprio vantaggio

Per tali ragioni ECB è raramente usato.

### 3.2.2 Cipher Block Chaining (CBC)

CBC non presenta i problemi di ECB: a due blocchi in chiaro identici non corrispondono due blocchi cifrati identici.

#### Idea base

Per comprendere CBC conviene prima considerare il seguente esempio, in riferimento alla Figura 3.4 che ne condivide l'idea base:

- per ogni blocco di testo in chiaro  $m_i$  viene generato un numero random a 64 bit  $r_i$
- $m_i$  e  $r_i$  vengono sommati ( $\oplus$  XOR)
- il risultato viene cifrato con la chiave segreta
- i blocchi cifrati  $c_i$  e i numeri random, in chiaro,  $r_i$  vengono trasmessi

E per riottenere il testo in chiaro:

- vengono decifrati i blocchi  $c_i$  con la chiave segreta
- i blocchi risultanti vengono sommati ( $\oplus$  XOR) con i numeri random  $r_i$

L'esempio appena visto è molto inefficiente, infatti l'informazione da trasmettere è duplicata perché per ogni blocco va trasmesso il corrispondente numero random.

Un altro problema è che un avversario può riarrangiare i blocchi in modo da ottenere un effetto predittivo sul testo in chiaro, ad esempio:

- se la coppia  $r_2|c_2$  fosse rimossa il corrispondente blocco in chiaro  $m_2$  scomparirebbe
- se la coppia  $r_2|c_2$  fosse scambiata con la coppia  $r_7|c_7 \Rightarrow m_2$  e  $m_7$  risulterebbero scambiati
- se l'avversario conosce ciascun  $m_i$ , può modificare  $m_i$  in modo predittivo cambiando il corrispondente numero random  $r_i$

### Funzionamento

CBC genera i “propri” numeri random usando  $c_i$  come numero random  $r_{i+1}$ , cioè usa il precedente blocco cifrato come numero random da sommare ( $\oplus$  XOR) al blocco di testo in chiaro successivo.

Per evitare che due testi in chiaro inizialmente identici diano luogo a dei blocchi cifrati inizialmente identici CBC genera un singolo numero random, detto vettore di inizializzazione (**Initialization Vector IV**), che viene sommato ( $\oplus$  XOR) con il primo blocco di testo in chiaro. Il risultato viene trasmesso dopo la cifratura a chiave segreta.

La decifratura è semplice essendo l’or-esclusivo un’operazione che coincide con la propria inversa.

Quanto detto, rappresentato nelle figure Figura 3.5 e Figura 3.6, può essere espresso anche algebricamente:

- CIFRATURA
 
$$c_1 = E(K, (IV \oplus m_1))$$

$$c_i = E(K, (c_{i-1} \oplus m_i)) \forall i > 1$$
- DECIFRATURA
 
$$m_1 = E(K, c_1) \oplus IV$$

$$m_i = E(K, c_i) \oplus c_{i-1}$$

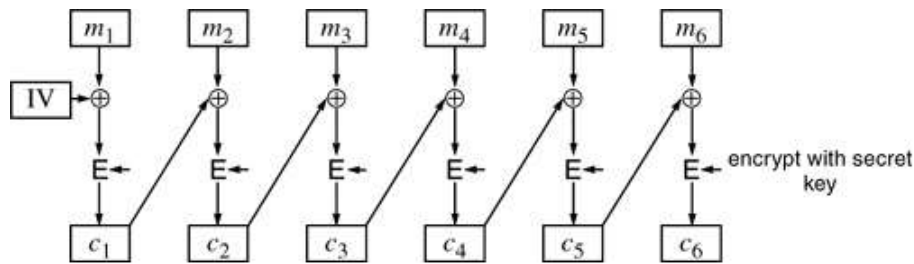


Figura 3.5: Schema di crittografia CBC

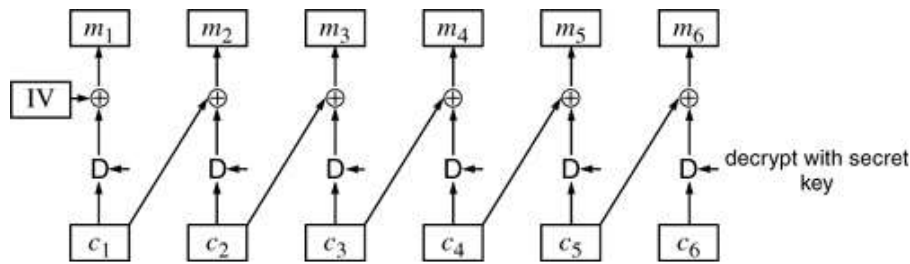


Figura 3.6: Schema di decrittografia CBC

Si noti che, essendo il costo della somma ( $\oplus$  XOR) trascurabile rispetto al costo della cifratura a chiave segreta, la cifratura con CBC ha le stesse prestazioni della cifratura con ECB eccetto il costo delle generazione e trasmissione di  $IV$ . In molti casi, tuttavia, la sicurezza di CBC non dipende dalla scelta del vettore di inizializzazione  $IV$  (cioè si possono anche porre tutte le cifre di  $IV$  pari a 0).

In alcuni casi, tuttavia, l’assenza di  $IV$  riduce la sicurezza. Ad esempio, si supponga che il file cifrato contenente i salari dei dipendenti sia trasmesso settimanalmente; in assenza di  $IV$ , un ascoltatore potrebbe verificare se il testo cifrato differisce da quelle della precedente settimana, e potrebbe determinare la prima persona il cui salario è cambiato. Un altro esempio è quello di un generale che invia giornalmente delle informazioni segrete dicendo “continue holding your position”; il testo cifrato sarebbe ogni giorno lo stesso, finché il generale decide di cambiare ordine, inviando il messaggio “start bombing”: il testo cifrato cambierebbe immediatamente, allertando

il nemico.

Un vettore di inizializzazione scelto randomicamente garantisce che, anche se lo stesso messaggio è inviato ripetutamente, il corrispondente testo cifrato risulta ogni volta differente, e previene attacchi all'algoritmo di cifratura di tipo testo in chiaro selezionato anche quando un avversario può fornire del testo in chiaro al CBC.

### CBC minaccia 1 – Modifica dei blocchi cifrati

L'uso di CBC non elimina il problema che qualcuno possa modificare il messaggio in transito, semplicemente cambia la natura della minaccia: un avversario non può più vedere ripetizioni di blocchi cifrati, e non può più copiare/spostare blocchi cifrati (ad esempio per scambiare il salario di due dipendenti) ma può ancora modificare il testo cifrato in modo predittivo.

Cosa potrebbe succedere se modificasse un blocco di testo cifrato, ad esempio  $c_n$ ?

Da  $m_{n+1} = E(K, c_{n+1}) \oplus c_n$  si evince che una modifica di  $c_n$  può avere un effetto prevedibile su  $m_{n+1}$  (ad esempio, cambiando il terzo bit di  $c_n$  cambia il terzo bit di  $m_{n+1}$ ); chiaramente essendo anche  $m_n = E(K, c_n) \oplus c_{n-1}$ , l'avversario non può prevedere quale possa essere il nuovo valore di  $m_n$ , molto probabilmente la modifica di  $c_n$  corrompe completamente il blocco in chiaro  $m_n$ .

Vediamo a tal proposito l'esempio seguente, illustrato in Figura 3.7:

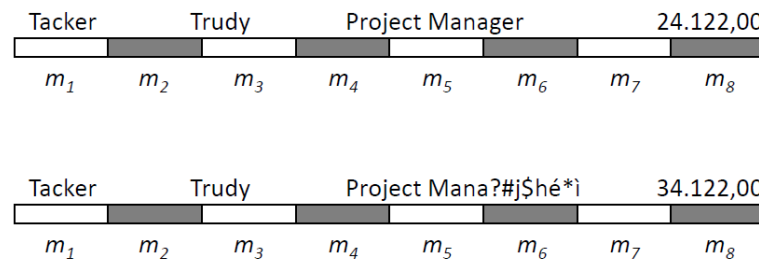


Figura 3.7: Modifica dei blocchi cifrati

Supponiamo che un avversario (Trudy) sappia che una data sequenza di blocchi cifrati, del file dei salari, corrispondano alla riga contenente i suoi dati personali; se Trudy vuole aumentare il suo salario di 10K, e se sa che l'ultimo byte di  $m_7$  corrisponde alle decine di migliaia nella codifica decimale (00000010), per darsi 10K in più deve semplicemente cambiare il bit meno significativo di  $c_6$ ; da  $m_7 = D(K, c_7) \oplus c_6$  tuttavia, Trudy non sarà più in grado di predire cosa apparirà nella voce "Posizione", infatti, da  $m_6 = D(K, c_6) \oplus c_5$ , si vede che è impraticabile prevedere l'effetto della modifica di  $c_6$  su  $m_6$ . Se il file decifrato fosse letto da una persona umana, questa potrebbe insospettirsi della presenza di simboli strani nel campo "Posizione", se invece il file decifrato viene elaborato da un programma l'attacco potrebbe non essere rilevato.

Ricapitolando: Trudy è stato in grado di modificare un blocco in modo predittivo con l'effetto collaterale di modificare il blocco precedente senza poter prevedere il risultato finale.

### CBC minaccia 2 – Riarrangiamento blocchi cifrati

Con riferimento alla Figura 3.8, si supponga che Trudy conosca il testo in chiaro e, il corrispondente testo cifrato di qualche messaggio, cioè  $m_1, m_2, \dots, m_n$  e  $IV, c_1, c_2, \dots, c_n$ ; in questo modo Trudy conosce automaticamente anche il blocco decifrato di ciascun  $c_i$ , da  $D(K, c_1) = c_{i-1} \oplus m_i$ . Da queste informazioni, Trudy può considerare ciascun  $c_i$  come un "building block" e costruire un flusso cifrato usando ogni combinazione di  $c_i$  ed essere in grado di calcolare quale sarà il corrispondente testo in chiaro.

Per capire a cosa potrebbe servire questo tipo di attacco si tenga presente che uno dei modi di combattere la minaccia di modifica di blocchi cifrati è includere un **CRC** (Cyclic Redundancy

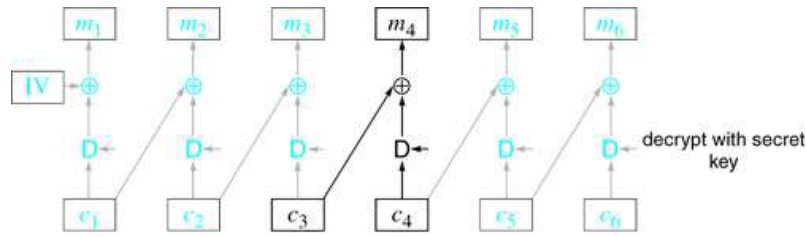


Figura 3.8: Riarrangiamento dei blocchi cifrati

Check) al testo in chiaro prima di cifrarlo con un CBC, perciò se Trudy modifica qualche blocco cifrato, il CRC consentirà ad un computer di rilevare prontamente l'alterazione del messaggio (e.g. se si fosse scelto un CRC a 32 bit ci sarebbe una possibilità su  $2^{32}$  che il CRC coincida con quello corretto); supponiamo che a Trudy non interessi quale possa essere il nuovo messaggio di testo in chiaro (che potrebbe essere completamente indecifrabile), ma interessi solamente che il nuovo messaggio manomesso sia accettato dal computer ricevente sapendo che viene eseguito un controllo di tipo CRC, Trudy può provare a costruire molti flussi cifrati combinando in modi diversi i blocchi  $c_1, c_2, \dots, c_n$  e può calcolare il risultante testo in chiaro per ciascuno di essi, per poi testare se il testo in chiaro risultante ha un CRC corretto (mediamente serviranno  $2^{31}$  tentativi).

Che male potrebbe fare Trudy modificando un messaggio, senza controllarne il contenuto, in modo tale che sia accettato dal computer ricevente? Forse Trudy è soltanto maliziosa, e vuole distruggere alcuni dati che vengono caricati attraverso la rete, ma in realtà, c'è un modo sottile di controllare, seppur in misura ridotta, il contenuto del messaggio modificato: supponiamo che Trudy sposti blocchi contigui, ad esempio, se  $c_n$  e  $c_{n+1}$  vengono spostati in qualche altro posto, allora il blocco originale  $m_{n+1}$  apparirà in un'altra posizione; se  $m_{n+1}$  contiene il salario del presidente, Trudy potrebbe scambiare i blocchi in modo da cambiarlo con il suo, ma poi dovrà modificare molto probabilmente gran parte del messaggio restante per garantire che il CRC risulti invariato.

Per prevenire attacchi di questo tipo, basati sul riarrangiamento dei blocchi cifrati e tali da preservare il CRC originario, potrebbe essere usato un CRC a 64 bit: ciò è sicuramente sufficiente se l'attacco al CRC, nell'ambito di un CBC, è di tipo a forza bruta.

Per chi progetta protocolli crittografici sicuri, una modalità di cifratura ad un singolo step che protegga sia la confidenzialità che l'autenticità di un messaggio è stata per molti anni una sorta di "Sacro Graal" da ricercare!

### 3.2.3 Output FeedBack Mode (OFB)

L'OFB è un cifrario a flusso: la cifratura consiste nel sommare ( $\oplus$  XOR) il messaggio con il keystream (o one-time pad) generato da OFB stesso. Supponiamo che il keystream sia ottenuto generando singoli blocchi di 64 bit alla volta; un possibile modo per generarlo è il seguente:

- viene generato un numero random  $IV$  (Initialization Vector) di 64 bit
- il primo blocco del keystream coincide con  $IV$ :  $b_0 = IV$
- i blocchi seguenti  $b_i$  si ottengono cifrando  $b_{i-1}$  con la chiave segreta:  $b_i = E(K, b_{i-1})$

Il one-time pad (keystream) risultante è dato dalla sequenza  $OTP = OTP(K, IV) = b_0|b_1|b_2|\dots|b_i|b_{i+1}|\dots$ .

La cifratura con OFB (Figura 3.9) consiste nel sommare ( $\oplus$  XOR) il messaggio  $m$  con OTP, se  $m$  ha lunghezza  $l_m$  bit si considereranno soltanto  $l_m$  bit di OTP. Il risultato della cifratura  $c = OTP \oplus m$  viene trasmesso insieme a  $IV$  (la lunghezza  $l_c$  di  $c$  coincide con  $l_m$ ).

In decifratura (Figura 3.10) il destinatario riceve  $IV$  e conoscendo  $K$  calcola lo stesso onetime pad  $OTP = OTP(K, IV)$  il messaggio  $m$  si ottiene sommando ( $\oplus$  XOR) il flusso cifrato  $c$  con  $l_c$  bit di OTP.

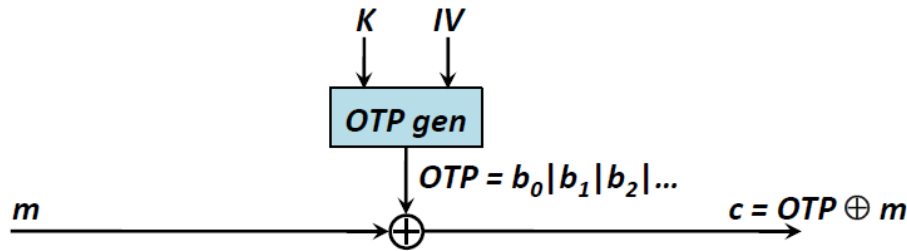


Figura 3.9: Schema di crittografia OFB

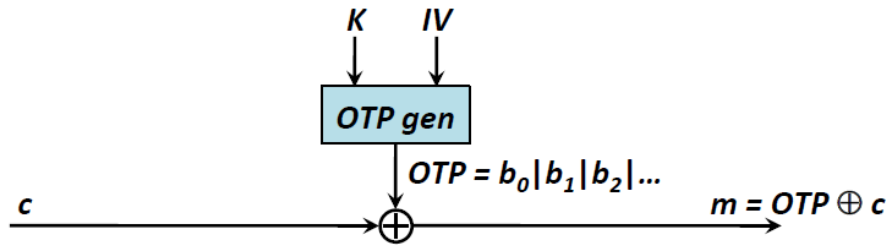


Figura 3.10: Schema di decrittografia OFB

### Vantaggi e svantaggi di OFB

OFB presenta i seguenti vantaggi:

- visto che il one-time pad OTP può essere generato in anticipo, prima che sia noto il messaggio  $m$  da cifrare, una volta ottenuto  $m$  è necessario soltanto effettuare la somma ( $\oplus$  XOR) con il one-time pad (lo XOR è eseguibile in modo estremamente veloce)
- se qualche bit del testo cifrato dovesse corrompersi, soltanto i corrispondenti bit del testo in chiaro sarebbero corrotti, diversamente dalla modalità CBC, dove se  $c_n$  fosse corrotto allora  $m_n$  sarebbe completamente corrotto e  $m_{n+1}$  sarebbe corrotto in corrispondenza dei medesimi bit di  $c_n$
- un messaggio  $m$  può arrivare a pezzi di lunghezza arbitraria, e, ogni volta che arriva un pezzo, il corrispondente testo cifrato può essere immediatamente trasmesso; in CBC invece, se il messaggio arriva un byte alla volta, per la cifratura è comunque necessario attendere che un blocco di 64 bit (o un multiplo intero di 8 byte) sia completo (ciò può comportare l'attesa di altri 7 byte o l'aggiunta di bit di riempimento, cosa che aumenta la quantità di dati da trasmettere)

OTP ha però anche il seguente svantaggio:

- se un avversario conoscesse il testo in chiaro  $m$  e quello cifrato  $c$ , potrebbe modificare il testo in chiaro a piacimento semplicemente sommando il testo cifrato con il testo in chiaro noto, e sommando il risultato con un qualsiasi messaggio  $m'$  che desidera sostituire ad  $m$ ; cioè l'avversario dovrebbe modificare il testo cifrato come  $c' = c \oplus m \oplus m'$  e verificare che decifrando  $c'$  anziché  $c$  si ottiene  $m'$  anziché  $m$ .

### 3.2.4 k-bit Output FeedBack Mode (k-OFB)

In generale la modalità OFB consente di generare flussi di "pezzi" da  $k$  bit (quanto visto prima corrisponde al caso in cui  $k = 64$  bit). La modalità k-bit OFB funziona nel seguente modo (si descriverà la versione data in [DES81]) con riferimento alla Figura 3.11:

- l'input  $I_0$  al modulo di cifratura DES è inizializzato a  $IV$ , cioè  $I_0 = IV$ : se  $IV$  ha meno di 64 bit, vengono inseriti degli 0 di riempimento a sinistra (cifre più significative)



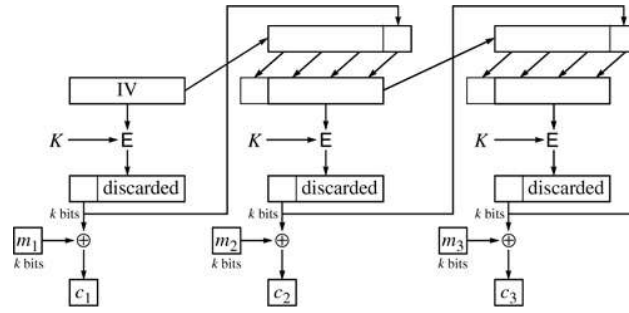


Figura 3.11: k-bit OFB

- il primo pezzo  $b_0$  di OTP si ottiene selezionando  $k$  bit dall'output  $O_0 = E(K, I_0)$  di DES (una quantità a 64 bit); da un punto di vista crittografico non ha importanza come siano scelti tali bit da  $O_0$ ; [DES81] specifica che devono essere i  $k$  bit più significativi
- l' $i$ -esimo pezzo  $b_i$  si ottiene selezionando i  $k$  bit più significativi dell'output  $O_i = E(K, I_i)$  di DES, ove l'input  $I_i$  è stato ottenuto da  $I_{i-1}$  eseguendo una traslazione a sinistra di  $k$  bit, e un inserimento di  $b_{i-1}$  nei  $k$  bit meno significativi di  $I_1$  ( $k$  bit più a destra)

### 3.2.5 Cipher FeedBack Mode (CFB)

La modalità CFB è molto simile a OFB, con riferimento alla Figura 3.12:

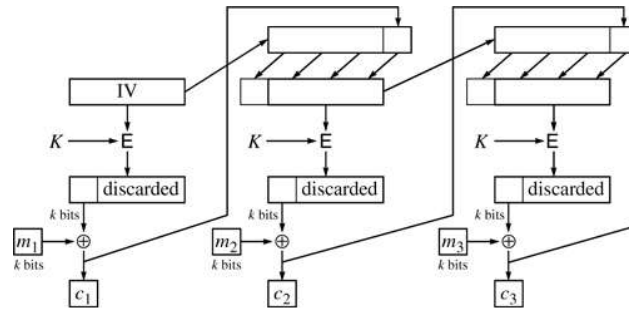


Figura 3.12: k-bit CFB

- viene prodotto un one-time pad generando, uno alla volta, singoli pezzi di  $k$  bit
- il one-time pad viene sommato ( $\oplus$  XOR) con pezzi di  $k$  bit del messaggio

Si noti che in OFB i  $k$  bit meno significativi dell'input  $I_i$  del modulo di cifratura DES sono i  $k$  bit di  $b_{i-1}$  (sono parte dell'output  $O_{i-1}$  della cifratura DES del blocco precedente; invece, in CFB i  $k$  bit di  $I_i$  sono i  $k$  bit di testo cifrato del blocco precedente, cioè i  $k$  bit di  $c_{i-1}$  (in CFB il one-time pad non può essere generato prima che il messaggio è noto, a differenza di OFB), nella modalità a  $k$ -bit è ragionevole assegnare a  $k$  un valore diverso da 64 bit (una scelta sensata è  $k = 8$  bit).

#### Vantaggi e svantaggi di CFB

CBF presenta i seguenti vantaggi:

- Con OFB o CBC, se si ha una perdita di caratteri in trasmissione (testo cifrato), i.e. se nel flusso cifrato  $c_1, c_2, c_3, \dots, c_n, \dots$  si perde il carattere  $c_k$ , allora a destinazione si ottiene la sequenza  $c_1, c_2, c_3, \dots, c_{k'}, \dots, c_{n-1'}$  ove  $c_{k'} = c_{k+1}, c_{k+1'} = c_{k+2}, \dots, c_{k+i'} = c_{k+i+1}$ ; oppure, con OFB o CBC, se extra caratteri sono aggiunti al flusso cifrato, i.e. se nel flusso

cifratoc<sub>1</sub>, c<sub>2</sub>, c<sub>3</sub>, ..., c<sub>n</sub>, ... si aggiunge il carattere c\* dopo di c<sub>k-1</sub>, allora a destinazione si ottiene la sequenza c<sub>1</sub>, c<sub>2</sub>, c<sub>3</sub>, ..., c<sub>k'</sub>, ..., c<sub>n+1'</sub> ove c<sub>k'</sub> = c\*, c<sub>k+1'</sub> = c<sub>k</sub>, ..., c<sub>k+i'</sub> = c<sub>k+i-1</sub>. Quindi l'intera parte restante della trasmissione risulta indecifrabile poiché m<sub>i'</sub> = c<sub>i'</sub> ⊕ b<sub>i</sub> e b<sub>i</sub> = b<sub>i</sub>(K, IV) cioè b<sub>i</sub> non dipende dalla sequenza cifrata. Invece, con 8-bit CFB, si ha un effetto risincronizzante: se un byte ci è perso in trasmissione allora corrispondente testo in chiaro mi è perso, e i successivi 8 byte m<sub>i+1</sub>, ..., m<sub>i+8</sub> risulteranno indecifrabili, ma dal byte m<sub>i+9</sub> in poi il testo in chiaro sarà corretto, questo perché b<sub>i</sub> = b<sub>i</sub>(K, c<sub>i-1</sub>), cioè b<sub>i</sub> è derivato dalla sequenza di caratteri cifrati. Discorsi analoghi valgono nel caso dell'aggiunta di un byte al flusso cifrato.

- i messaggi cifrati con CFB offrono più protezione di CBC e di OFB rispetto ad eventuali manomissioni; infatti, nel caso di 8-bit CFB un avversario può modificare ogni singolo byte in modo predittivo, ma con l'effetto collaterale di non poter prevedere/controllare i successivi 8 byte discorsi simili valgono per 64-bit CFB.
- a differenza di CBC, non sono possibili attacchi basati sul riarrangiamento di blocchi; tuttavia intere sezioni del messaggio possono essere riarrangiate rendendo indecifrabili le parti corrispondenti ai "punti di giuntura".

CBF ha anche i seguenti svantaggi:

- 8-bit CFB ha lo svantaggio che ogni byte di input richiede un'operazione DES. Inizialmente CFB fu concepito per essere utilizzato con un numero arbitrario k di bit per "pezzo", con k minore della dimensione di un blocco completo (64 bit per DES); nella pratica tuttavia k è pari a 1 byte oppure coincide con la dimensione piena (full-block) dei blocchi del modulo di cifratura. Quando utilizzato in modalità full-block le prestazioni di CFB sono comparabili a quelle di ECB, CBC, e OFB.
- come OFB consente di cifrare ed inviare ciascun byte del messaggio non appena è noto tuttavia, a differenza di OFB non è in grado di anticipare il calcolo del one-time pad in fine, è in grado di rilevare delle alterazioni meglio di OFB, ma non bene quanto CBC.

### 3.2.6 CounTeR Mode (CTR)

CTR (Figura 3.13) è simile a OFB perché un one-time pad viene generato e sommato (⊕ XOR) con i dati; tuttavia differisce da OFB perché non concatena ciascun blocco di one-time-pad con il precedente, ma incrementa IV e poi cifra quanto ottenuto per ottenere il prossimo blocco di one-time pad.

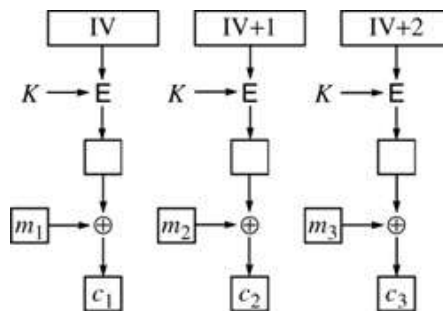


Figura 3.13: CTR

### 3.2.7 Vantaggi e svantaggi di CTR

Il vantaggio principale di CTR è che, come OFB, il one-time pad può essere pre-calcolato, e la cifratura consiste in un semplice XOR; inoltre, come in CBC, la decifratura di un messaggio può iniziare da un qualunque blocco (non è obbligata ad iniziare dal primo blocco). Per questo CRT

è l'ideale in applicazioni che richiedono la cifratura di file/memorie ad accesso casuale (sottoinsiemi di dati prelevati ed ordine non prevedibili).

Come in OFB (e in tutti i cifrari a flusso), nella modalità CTR si ha una perdita di sicurezza se messaggi diversi sono cifrati con la stessa coppia  $\langle K, IV \rangle$ , poichè un avversario potrebbe ottenere la somma ( $\oplus$  XOR) dei testi in chiaro se somma ( $\oplus$  XOR) due testi cifrati ottenuti con la stessa coppia  $\langle K, IV \rangle$ .

### 3.3 Generare message authentication code(MAC)

Un sistema di cifratura a chiave segreta può essere usato per generare un MAC cioè un checksum cifrato: **MAC** sta per **M**essage **A**uthentication **C**ode.

Un sinonimo di MAC è **MIC** (**M**essage **I**ntegrity **C**ode) e, anche se il termine MAC è più popolare; nella **PEM** (**P**rivacy **E**nhanced **M**ail) viene usato il termine MIC.

Le modalità operative CBC, CFB, OFB, e CTR offrono una buona protezione della confidenzialità, i.e. un messaggio intercettato è difficilmente decifrabile, ma non offrono una buona protezione dell'integrità/autenticità di un messaggio, i.e. non proteggono da ascoltatori che lo modificano in modo non rilevabile.

Nel seguito useremo i termini integrità e autenticità in modo intercambiabile visto che se il messaggio è integro allora non è stato modificato dal momento in cui è stato generato, i.e. il messaggio è autentico.

#### 3.3.1 Residuo CBC

Un modo standard per assicurare l'autenticità di un messaggio  $m$  (cioè per proteggersi da modifiche di  $m$  non rilevabili) è, in riferimento alla Figura 3.14 :

- calcolare il CBC di  $m$
- inviare soltanto l'ultimo blocco cifrato (64 bit) e il messaggio  $m$  in chiaro; l'ultimo blocco cifrato è detto **residuo CBC**.

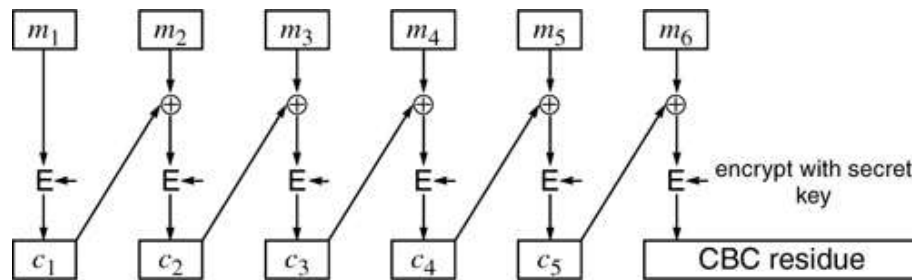


Figura 3.14: Residuo CBC

Il calcolo del residuo CBC richiede la conoscenza della chiave segreta  $K$ , quindi se un avversario modifica  $m$  in  $m'$  allora  $res_{CBC}(m')$  sarà diverso da  $res_{CBC}(m)$  (c'è solo 1 possibilità su  $2^{64}$  che siano uguali) perchè l'avversario non è in grado di calcolare  $res_{CBC}(m')$  senza conoscere la chiave segreta  $K$ .

Il destinatario del messaggio calcola il residuo del messaggio in chiaro ricevuto, e verifica che sia uguale al residuo ricevuto; se i residui coincidono deduce che (con elevata probabilità) il residuo ricevuto è stato calcolato da qualcuno che conosce la chiave segreta, i.e. il mittente è autentico.

In molte applicazioni non è necessario proteggere la confidenzialità, ma solo l'autenticità; in questi casi si può trasmettere il testo in chiaro più il residuo. Tuttavia, è assai frequente la

necessità di proteggere contemporaneamente confidenzialità e autenticità: se il messaggio  $m$  è un singolo blocco, ciò può ottenersi con una semplice cifratura a chiave segreta. Nel caso di un messaggio multi blocco qual è la trasformazione equivalente?

### 3.3.2 Assicurare confidenzialità e autenticità

Dato un messaggio  $m$ :

- per assicurare la **confidenzialità** di  $m$  basta cifrarlo in modalità CBC
- per assicurare l'**autenticità** di  $m$  basta inviare  $res_{CBC}(m)$  più  $m$  in chiaro

Allora a prima vista la soluzione riportata in Figura 3.15 sembrerebbe assicurare confidenzialità e autenticità: In realtà tale soluzione è chiaramente errata, infatti consiste nell'inviare il mes-

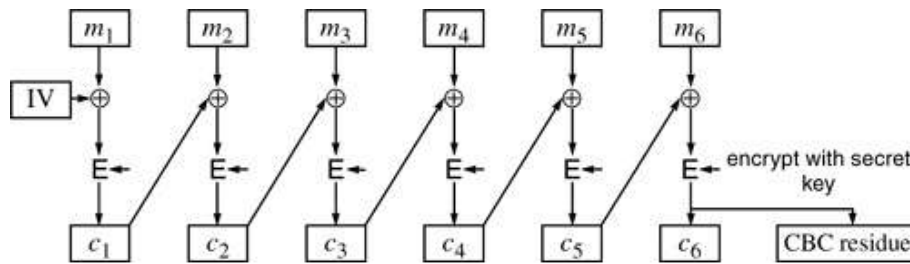


Figura 3.15: Assicurare confidenzialità e autenticità: soluzione 1

saggio cifrato nella modalità CBC ( $E_{CBC}(K, IV, m)$ ) ripetendo soltanto l'ultimo blocco cifrato ( $res_{CBC}(m)$ ); così chiunque voglia alterare il messaggio deve solo modificare uno o più blocchi cifrati con CBC e inviare il nuovo messaggio ripetendo due volte l'ultimo blocco cifrato. Quindi inviare il residuo CBC in aggiunta al messaggio cifrato con CBC non aumenta la sicurezza.

Si noti infatti che per autenticità (integrità) intendiamo che un calcolatore è in grado di rilevare automaticamente se il messaggio è stato alterato. Usando CBC da solo, allora, non è possibile rilevare in modo automatico eventuali modifiche di un messaggio, poiché ogni stringa di bit, comunque venga generata, viene decifrata in "qualcosa", e gli ultimi 64 bit di quella stringa sono il suo residuo CBC corretto; in questo modo chiunque intercetti il testo cifrato può modificarlo, e un computer a destinazione decifrerà il risultato, che potrebbe essere assolutamente privo di senso, senza essere consapevole che quanto ottenuto è di fatto spazzatura.

Un utente umano si renderebbe conto che il testo cifrato è stato alterato, a meno che la modifica non sia stata eseguita da un avversario in modo "pulito", ma un computer non è in grado di farlo se non si aggiunge un controllo di integrità.

Un'alternativa potrebbe essere calcolare il residuo CBC del messaggio  $res_{CBC}(m)$ , allegarlo al testo in chiaro  $m$ , e cifrare con CBC la concatenazione  $m|res_{CBC}(m)$  (Figura 3.16) In realtà

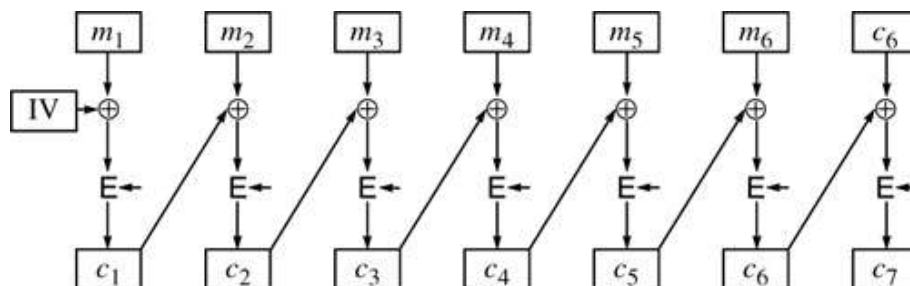


Figura 3.16: Assicurare confidenzialità e autenticità: soluzione 2

neanche questa soluzione funziona, infatti:  $c_7 = res_{CBC}(m) = E(K, c_6 \oplus c_6) = E(K, 000 \dots 0)$ , cioè il residuo CBC è una stringa ottenuta cifrando con la chiave segreta una stringa di 64 bit a 0, quindi il residuo CBC non dipende da  $m$  e non può offrire alcuna protezione di integrità.

Come altra alternativa, supponiamo di calcolare un checksum non crittografico  $CRC(m)$  (ad esempio, un CRC) del messaggio  $m$  e di appenderlo alla fine di  $m$ , e di cifrare con CBC il tutto:  $m|CRC(m)$ , secondo lo schema in Figura 3.17 Questa soluzione "quasi" funziona: è vulnerabile

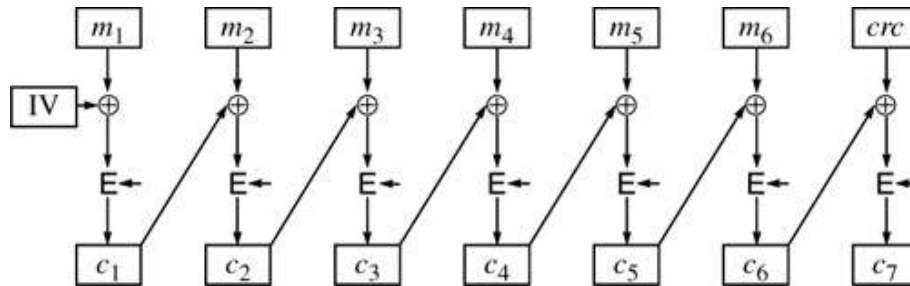


Figura 3.17: Assicurare confidenzialità e autenticità: soluzione 3

ad attacchi molto sottili se il CRC è corto, d'altro canto checksum non crittografici più lunghi sono "sospetti".

### Soluzione sicura

Viene considerata una soluzione sicura quella che riesce a proteggere la confidenzialità di un messaggio  $m$  cifrandolo con CBC, e l'integrità di  $m$  con un residuo CBC, a patto che vengano usate due chiavi distinte,  $K$  e  $K'$ :

- confidenzialità:  $E_{CBC}(K, IV, m)$
- integrità:  $res_{CBC}(K', IV, m)$

Chiaramente ciò comporta una notevole perdita di efficienza, infatti il costo computazionale è duplicato rispetto al costo della sola cifratura CBC.

Sono state proposte tecniche più rapide, ma generalmente presentano sempre dei "sottili difetti" crittografici (se tali difetti siano seri o meno dipende dal tipo di applicazione e dall'intelligenza dell'avversario); alcune di queste tecniche sono:

- **CBC con un Checksum Crittografico Debole:** Visto che l'uso di checksum non crittografici in CBC risulta poco sicuro, e che checksum crittografici di qualità sono computazionalmente dispendiosi, è stato proposto di usare checksum crittografici "deboli". Complessivamente dovrebbe essere una soluzione sicura, infatti lo sforzo computazionale per violare il checksum debole va moltiplicato per le limitazioni derivanti dal fatto che è usato in una cifratura CBC. Sebbene non ci sono ragioni per sostenere che tale schema sia insicuro, CBC con checksum crittografici deboli non ha riscosso successo (si consideri che Kerberos IV usa un checksum crittografico debole per la protezione d'integrità fuori da uno schema di cifratura e sembra che non sia mai stato violato!)
- **Cifratura CBC e Residuo CBC con Chiavi Correlate:** anziché usare due chiavi completamente indipendenti per la cifratura CBC e per il calcolo del residuo, un trucco usato in Kerberos V è impiegare una versione modificata della chiave in una delle due operazioni. Cambiare un singolo bit dovrebbe essere sufficiente, ma Kerberos invece somma ( $\oplus$  XOR) la chiave con la costante a 64 bit  $F0F0F0F0F0F0F0F0_{16}$ ; tale soluzione preserva la parità della chiave e non trasforma mai una chiave non-debole in una chiave debole. Il fatto di avere una chiave matematicamente correlata all'altra (in alternativa alla scelta di due numeri random come chiavi) non introduce particolari debolezze, ma non introduce

neanche particolari vantaggi (in generale, distribuire una coppia di chiavi non è più difficile di distribuirne solo una, e il fatto che due chiavi siano matematicamente correlate non riduce il carico computazionale, l'unico vantaggio nel derivare una chiave dall'altra lo si ha quando si dispone di un sistema/servizio per la distribuzioni di chiavi singole che non è estendibile al caso di coppie di chiavi).

- **CBC con Hash Crittografico:** un altro approccio è concatenare un messaggio  $m$  con il suo hash crittografico  $h(m)$ , tipicamente 128 bit, e cifrare con CBC il tutto,  $m|h(m)$ . Tale soluzione è probabilmente sicura, sebbene non sia stata adeguatamente studiata, visto che gli schemi moderni usano hash cifrati con chiavi richiede due fasi crittografiche (come nel caso della cifratura CBC più il residuo CBC con chiavi distinte), ma è più efficiente se la funzione di hash è più veloce dell'algoritmo di cifratura
- **Offset Codebook Mode (OCB):** OCB è uno dei molti modi che permette di ottenere cifratura e protezione di integrità effettuando soltanto una singola fase di cifratura. OCB e altre tecniche simili sono molto recenti per avere un supporto di studi e test, spesso sono gravate da licenze/patenti, ma sembra molto probabile che una o più di queste tecniche diventi alla fine il modo standard per ottenere protezione di integrità e di confidenzialità.

### 3.4 Cifratura multipla DES

#### 3.4.1 Cifratura multipla EDE o 3DES

In generale, ogni schema di cifratura può essere reso più sicuro ricorrendo alla cifratura multipla. Nel caso di DES, è universalmente ritenuta sicura la procedura nota come EDE. **Encrypt-Decrypt-Encrypt** (o 3DES, **triplo DES**):

- $c = E(K_1, D(K_2, E(K_1, m))) = (E_1 \circ D_2 \circ E_1)(m)$
- $m = D(K_1, E(K_2, D(K_1, c))) = (D_1 \circ E_2 \circ D_1)(c)$

La cifratura multipla EDE è di fatto un meccanismo per incrementare la lunghezza della chiave DES. Sebbene sia stata introdotta per arrivare ad uno standard sicuro basato su DES, in linea di principio è applicabile anche ad altri schemi di cifratura, ed esempio ad IDEA, ma è più importante nel caso di DES poiché la chiave DES è notoriamente considerata troppo corta.

Si è visto che uno schema di crittografia presenta sempre due funzioni, note come cifratura e decifratura; tali funzioni sono l'una l'inversa dell'altra, i.e.: ciascuna prende in input un blocco di dati  $m$ , e restituisce il corrispondente blocco offuscato  $c$  tale che, applicando a  $c$  l'altra funzione si ottiene  $m$ . Ha quindi senso applicare la "funzione di decifratura"  $D(K, m)$  al testo in chiaro  $m$  per cifrarlo e poi applicare la "funzione di cifratura"  $E(K, D(K, m))$  per decifrare quanto ottenuto riottenendo il testo in chiaro  $m$ ; ma in definitiva ha poco senso chiamare  $E(K, m)$  "funzione di cifratura", e  $D(K, m)$  "funzione di decifratura", poiché i ruoli di tali funzioni sono interscambiabili. Conviene chiamarle semplicemente **funzione**  $E()$  e **funzione**  $D()$  (tuttavia, spesso si continuerà a chiamarle funzione di cifratura e funzione di decifratura).

Realizzare una cifratura multipla non è banale, specie se si desidera anche ottenere un cifrario a flusso a partire da un cifrario a blocchi.

Il metodo standard per usare EDE è il seguente: vengono usate due chiavi (e non tre),  $K_1$  e  $K_2$  e ogni blocco di testo in chiaro  $m_i$  è sottoposto prima ad  $E_1()$  (cioè viene eseguito  $E(K_1, m_i)$ ), poi a  $D_2()$  (cioè viene eseguito  $D(K_2, E(K_1, m_i))$ ) e in fine ancora ad  $E_1()$  (cioè viene eseguito  $E(K_1, D(K_2, E(K_1, m_i)))$ ).

Quanto ottenuto è di fatto un nuovo schema di cifratura a chiave segreta (Figura 3.18): un blocco di 64 bit in input è mappato in un altro blocco di 64 bit in output; il processo è invertibile se si conoscono le chiavi, altrimenti è di fatto impraticabile risalire dall'output all'input. La decifratura EDE è semplicemente il processo inverso (Figura 3.19):

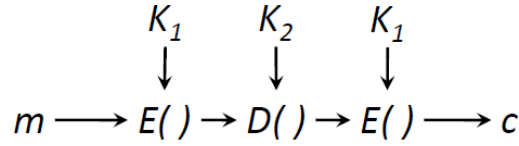


Figura 3.18: Cifratura EDE o 3DES

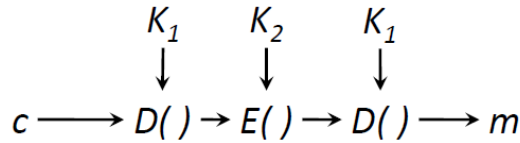


Figura 3.19: Decifratura EDE

### 3.4.2 EDE con CBC Outside/Inside

Per ottenere un cifrario a flusso (i.e. la corrispondente modalità operativa di flusso) a partire dal cifrario a blocchi EDE, viene usata la modalità operativa **CBC outside**, i.e. le tre funzioni  $E_1() - D_2() - E_1()$  vengono applicate a ciascun blocco, ma il concatenamento CBC viene eseguito soltanto una volta (Figura 3.20).

Il cifrario a flusso è ottenibile anche con un concatenamento **CBC inside**, i.e. si considerano una

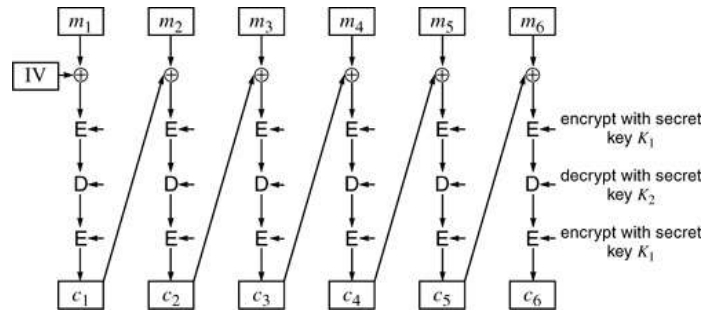


Figura 3.20: EDE con CBC Outside

cascata di tre concatenamenti CBC (semplificando alcuni passaggi): prima utilizzando  $CBC - E_1()$ , poi utilizzando  $CBC - D_2()$  e infine utilizzando ancora  $CBC - E_1()$  (Figura 3.21).

#### CBC Outside vs Inside

Il 3DES comunemente usato nelle applicazioni esegue un concatenamento CBC esterno: ad ogni blocco viene applicata la cifratura tripla e il concatenamento CBC viene fatto una sola volta sui blocchi cifrati. L'alternativa sarebbe cifrare completamente il messaggio con  $K_1$  e CBC, poi decifrare il risultato con  $K_2$  e CBC, e in fine cifrare di nuovo quanto ottenuto con  $K_1$  (CBC interno).

Quali sono le implicazioni di queste scelte?

Si è visto che con CBC è possibile fare una modifica predittiva sul testo in chiaro  $m_n$  (ad esempio invertire il bit  $x$ ) invertendo il bit  $x$  nel blocco cifrato  $c_{n-1}$ ; ciò comporta però l'effetto collaterale di modificare in modo imprevedibile il blocco  $m_{n-1}$ , la possibilità di sfruttare questa debolezza dipende dal tipo di applicazione.

Con CBC esterno, un avversario può ancora sferrare questo tipo di attacco (il fatto che la cifratura è fatta con un triplo DES è del tutto influente): un avversario che inverte il bit  $x$  di un blocco cifrato  $c_{n-1}$  modificherà completamente e in modo imprevedibile il blocco di testo in

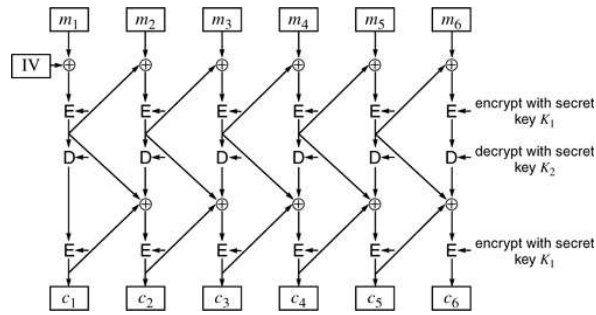


Figura 3.21: EDE con CBC Inside

chiaro  $m_{n-1}$  (il blocco di testo in chiaro  $m_n$  avrà il bit  $x$  invertito e tutti i blocchi di testo in chiaro diversi da  $m_{n-1}$  e  $m_n$  saranno invariati).

Con CBC interno, una modifica ad un blocco cifrato  $c_n$  altera in modo imprevedibile tutti i blocchi di testo in chiaro dal blocco  $m_n$  fino alla fine del messaggio. Per questo CBC interno è più sicuro di CBC esterno, e forse dovrebbe essere la scelta migliore; tuttavia, in alcuni casi è preferibile che la modifica di un blocco cifrato non si propaghi completamente nel resto del messaggio, i.e. sarebbe preferibile che lo schema di cifratura sia autosincronizzante (dopo un piccolo numero di blocchi corrotti, il testo in chiaro inizierà ad essere nuovamente decifrato correttamente).

Un altro vantaggio di CBC interno riguarda l'efficienza: triplicando l'uso di hardware e pipeline per le cifrature si può ottenere complessivamente una velocità pari a quella di una singola cifratura (con CBC esterno ciò non è possibile).

CBC interno presenta comunque delle sottili vulnerabilità se un avversario può esaminare l'output e fornire del testo in chiaro scelto e  $IV$ .

Una ragione per la quale CBC esterno è più usato nonostante i suoi svantaggi è che la cifratura EDE può considerarsi a tutti gli effetti un nuovo schema di cifratura (a chiave segreta) a blocchi che usa una chiave di 112 bit, perciò può essere utilizzata con ciascun metodo di concatenamento (OFB, ECB, CFB, CTR e CBC).



## Capitolo 4

# Funzioni Crittografiche di Hash

### 4.1 Introduzione

Una funzione di hash (o semplicemente hash o message digest) è una funzione unidirezionale (o one-way).

- è una funzione perché prende in input un messaggio e produce un output che dipende dal messaggio :
  - $h: \{0, 1\}^* \rightarrow \{0, 1\}^b$
  - $\{0, 1\}^*$ : spazio delle stringhe binarie di lunghezza qualsiasi
  - $\{0, 1\}^b$ : spazio delle stringhe binarie di lunghezza  $b$  bit
  - è considerata unidirezionale (one-way) perché è impraticabile capire quale input corrisponda ad un dato output

Sia  $h()$  una funzione di hash, allora  $h()$  è una funzione di hash sicura se :

- resistenza alla preimmagine: fissato un hash  $h$  è computazionalmente impraticabile trovare un messaggio  $m$  tale che  $h(m) = h$
- resistenza alle collisioni: è computazionalmente impraticabile trovare due messaggi  $m_1$  e  $m_2$  aventi lo stesso digest  $h(m_1) = h(m_2)$ , le proprietà precedenti implicano la seguente
- resistenza alla seconda preimmagine: dato un messaggio  $m$ , è computazionalmente impraticabile trovare un messaggio  $m'$  avente lo stesso digest  $h(m) = h(m')$

Si useranno i termini hash e message digest in modo intercambiabile; la funzione di hash del NIST è chiamata SHA-1: Secure Hash Algorithm mentre l'acronimo MD degli algoritmi MD2, MD4 e MD5 sta per Message Digest. Tutti gli algoritmi di digest/hash basicalmente fanno la stessa cosa: prendono in input un messaggio di lunghezza variabile, e restituiscono in output una quantità avente lunghezza prefissata. Dato un messaggio  $m$ , il digest  $h(m)$  viene calcolato in modo deterministico. Tuttavia, l'output della funzione di hash dovrebbe apparire il più possibile casuale. Dovrebbe essere impossibile, senza applicare la funzione di hash, predire ogni porzione dell'output e per ogni sottoinsieme (di posizioni) di bit nel digest  $h(m)$  soltanto procedendo in modo esaustivo dovrebbe essere possibile ottenere due messaggi  $m_1$  e  $m_2$  tali che  $h(m_1)$  e  $h(m_2)$  presentino gli stessi bit in quelle posizioni. Perciò una funzione di hash sicura con  $n$  bit dovrebbe essere derivabile da una funzione di hash con più di  $n$  bit prendendo un arbitrario sottoinsieme di  $n$  bit dal digest più grande. Chiaramente, ci sono molti messaggi distinti che sono mappati in uno stesso digest  $h(m)$ ;  $m$  ha lunghezza arbitraria, mentre il digest  $h(m)$  ha una lunghezza prefissata, ad esempio 128 bit. Se  $m$  ha una lunghezza di 1000 bit e  $h(m)$  di 128 bit ci sono in media 2872 messaggi che sono mappati in uno stesso digest dopo molti tentativi, due messaggi aventi lo stesso digest si trovano sicuramente. Tuttavia, per “molti tentativi” si intende un numero talmente grande che è di fatto impossibile considerando una buona funzione di digest a 128 bit, è

necessario provare approssimativamente  $2^{128}$  possibili messaggi prima di ottenere un messaggio avente un particolare digest, o  $2^{64}$  messaggi prima di trovarne due aventi lo stesso digest ; trovare cioè due messaggi che collidono.

## 4.2 Esempio di Applicazioni

Un'applicazione delle funzioni di hash crittografiche è il calcolo dell'impronta digitale di un programma o di un documento di cui si desiderano monitorare eventuali modifiche : se il message digest  $h(p)$  del programma  $p$  è noto e se  $h(p)$  è memorizzato in modo sicuro (cioè non può essere modificato da utenti non autorizzati) allora nessun utente non autorizzato può modificare  $p$  senza essere scoperto perché non sarà in grado di trovare un diverso programma  $p'$  tale che  $h(p') = h(p)$ . Quindi sia  $h: \{0,1\}^* \rightarrow \{0,1\}^b$  una funzione di hash siano  $m_1, m_2, \dots, m_N$   $N$  messaggi arbitrariamente scelti in  $\{0,1\}^*$ .

**DOMANDA:** quanto deve valere  $N$  per avere una probabilità del 50% che due messaggi  $m_i, m_j$  abbiano lo stesso hash?

Una prima stima di  $N$  (affinché ci sia il 50% di possibilità di collisione), per difetto, è la seguente :

- $k = 2^b$ : numero totale di possibili hash
- $\frac{1}{k}$  : probabilità che una coppia di messaggi collida
- **Ipotesi:** gli eventi considerati sono mutuamente esclusivi

$$- \Pr\{h(m_i) = h(m_j) \text{ OR } h(m_p) = h(m_q)\} = \Pr\{h(m_i) = h(m_j)\} + \Pr\{h(m_p) = h(m_q)\}$$

A rigore tale ipotesi non è soddisfatta, molti eventi hanno intersezione non nulla, perciò la stima ottenuta della probabilità è per eccesso e ciò si traduce in una stima per difetto di  $N$  ( $\Pr\{E1 \text{ OR } E2\} = \Pr\{E1\} + \Pr\{E2\} - \Pr\{E1 \cap E2\}$ ). Si ha una probabilità del 50% se si considerano  $k/2$  coppie, perciò  $N(N-1)/2 = k/2$  e ipotizzando  $N \gg 1$  si ha  $N = k^{1/2} = 2^{b/2}$ .

Una seconda stima, più accurata di  $N$  è la seguente:

- $P$ : probabilità che almeno una coppia di messaggi collida
- $P^*$ : probabilità che tutte le coppie di messaggi abbiano digest diversi, quindi  $P = 1 - P^*$
- **Ipotesi:** gli eventi considerati sono indipendenti

$$- \Pr\{h(m_i) \neq h(m_j) \text{ AND } h(m_p) \neq h(m_q)\} = \Pr\{h(m_i) \neq h(m_j)\} * \Pr\{h(m_p) \neq h(m_q)\}$$

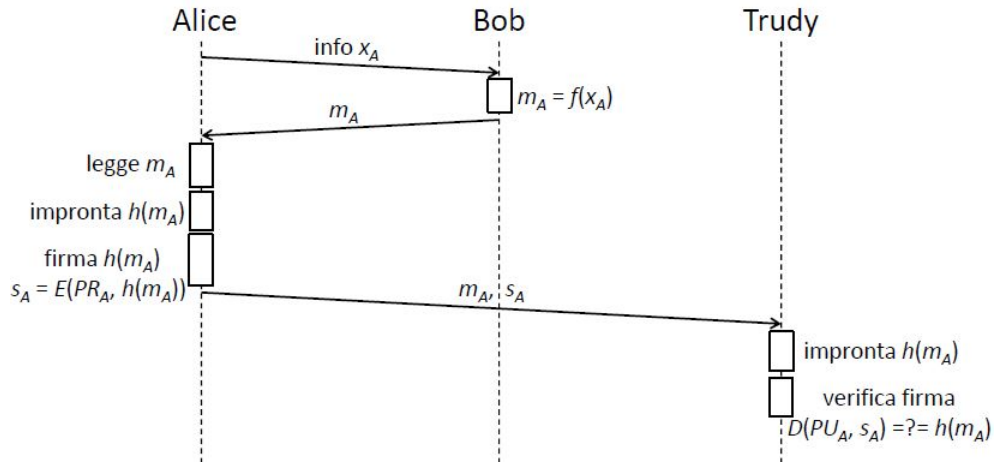
A rigore tale ipotesi non è soddisfatta, gli eventi non sono del tutto indipendenti quindi la stima ottenuta della probabilità  $P$  è per difetto e ciò si traduce in una stima per eccesso di  $N$  ( $\Pr\{E1 \text{ AND } E2\} = \Pr\{E1\} * \Pr\{E2\}$ ). Nella ipotesi di eventi indipendenti si ha  $P = 1 - P^* = 1 - (1 - 1/k)^{N(N-1)/2}$ , e ipotizzando che  $k \gg 1$  si ottiene che  $P \approx 1 - e^{-N(N-1)/2k}$ , ponendo pertanto  $P \geq 1/2$  si ottiene che  $e^{-N(N-1)/2k} \leq 1/2 = e^{-\ln 2}$ ; da cui si ottiene che  $N(N-1)/2 \geq (\ln 2)k$  e, ipotizzando che  $N \gg 1$ ,  $N \geq (2 \ln 2)^{1/2} \cdot k^{1/2} = (2 \ln 2)^{1/2} \cdot 2^{b/2}$ .

Una terza stima ancor più corretta si può ottenere utilizzando la modalità di calcolo utilizzata anche nel paradosso del compleanno :

- $P$ : probabilità che almeno una coppia di messaggi collida
- $P^*$ : probabilità che tutte le coppie di messaggi abbiano digest diversi, quindi  $P = 1 - P^*$
- $k = 2^b$ : numero di possibili hash

Si consideri inoltre la seguente notazione:

- $P_{2^*}$ : la probabilità che  $h(m_2)$  sia diverso da  $h(m_1)$
- $P_{3^*}$ : la probabilità che  $h(m_3)$  sia diverso da  $h(m_2)$  e  $h(m_1)$



- ...
- $P_{i*}$ : la probabilità che  $h(m_i)$  sia diverso da  $h(m_j)$ ,  $\forall 1 \leq j \leq i - 1$
- ...
- $P_{N*}$ : la probabilità che  $h(m_N)$  sia diverso da  $h(m_j)$ ,  $\forall 1 \leq j \leq N - 1$

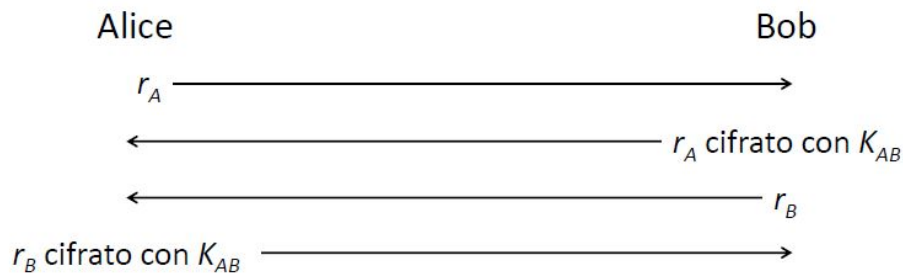
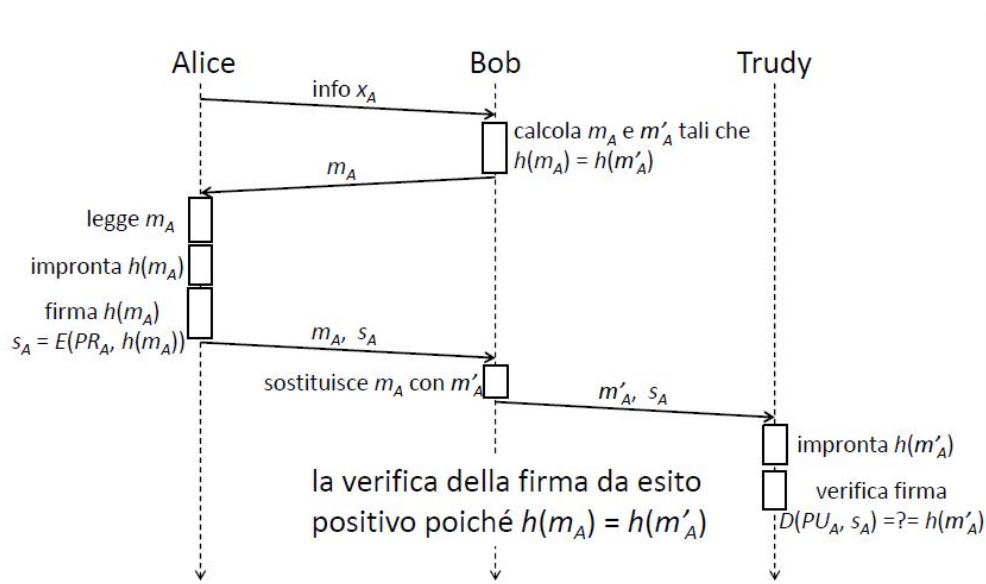
Da tutto ciò segue che  $P^* = P_{2*} * P_{3*} * \dots * P_{i*} * \dots * P_{N*} = (k-1)/k * (k-2)/k * \dots * (k-N+1)/k = \frac{k!}{(k^N * (k-N)!)} \Rightarrow P^* = \frac{k!}{(k^N * (k-N)!)}$ . Questa è la stima esatta di  $P^*$ , si nota che il precedente valore di  $P^*$  si può approssimare con  $1 \sim e^{-N(N-1)/2k}$ .

### 4.3 Lunghezza di un messaggio di Digest

Quanti bit deve avere l'output di una funzione di hash in modo tale che nessuno sia in grado di trovare due messaggi aventi lo stesso digest? Se il digest ha  $b$  bit, per trovare due messaggi aventi lo stesso digest, è necessario considerare circa  $2^{b/2}$  messaggi, se il digest è lungo 64 bit, la ricerca esaustiva in uno spazio di circa  $2^{32}$  elementi può essere fattibile mentre se il digest è lungo 128 bit si ritiene che una ricerca in uno spazio di  $2^{64}$  elementi sia impraticabile dato l'attuale stato dell'arte. Per quale ragione è importante che una funzione crittografica di hash sia resistente alle collisioni? Il fatto che debba essere resistente alla preeimmagine è scontato, ma la resistenza alle collisioni è veramente necessaria?? Sì, dato che in alcune circostanze riuscire a trovare due messaggi con lo stesso digest può comportare dei seri problemi di sicurezza!! Ad esempio, Alice genera una informazione  $x_A$  e incarica Bob di calcolare un messaggio  $m_A$  il cui contenuto deve dipendere da  $x_A$  secondo criteri prestabiliti. Una volta che Bob ha calcolato  $m_A$  lo sottopone ad Alice che ne verifica l'integrità e calcola l'impronta  $h(m_A)$ , la firma con la sua chiave privata e invia a Trudy il messaggio in chiaro  $m_A$  e la sua firma. Trudy legge il messaggio  $m_A$  e la firma, controlla che la firma sia quella di Alice e verifica che tutto  $m_A$  coincida con  $h(m_A)$ . Se la funzione non è resistente alle collisioni, Bob potrebbe trovare  $m_{A1}$  tale che risulti  $h(m_A) = h(m_{A1})$ . Una volta che Alice ha firmato il messaggio, sostituisce  $m_A$  con  $m_{A1}$  e Trudy non si potrà mai accorgere di nulla. Ma, per calcolare due messaggi con lo stesso hash, Bob può seguire il seguente approccio a forza bruta:

- dato  $x_A$ , calcola prima il messaggio  $m_A$  come desiderato da Alice;
- genera un messaggio falsato  $m_A'$ ;
- esegue il test  $h(m_A) == h(m_A')$ ;
- in caso negativo ritorna al punto 2;

con questo approccio a forza bruta, però, sono necessari circa  $2^b$  tentativi, e non  $2^{b/2}$ !



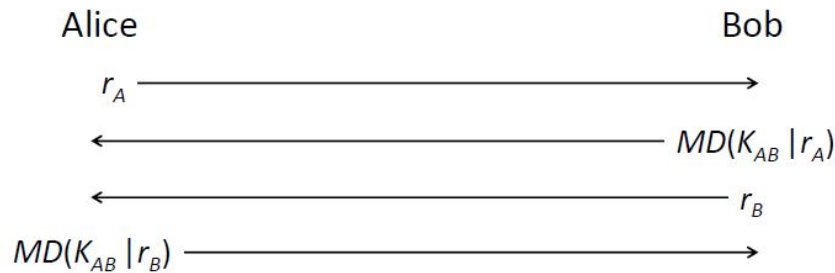
## 4.4 Impieghi degli Algoritmi di Hash

Disponendo di un segreto condiviso, l'algoritmo di hash può "sostituire" un algoritmo di crittografia a chiave segreta in ogni suo impiego. (Autenticazione a chiave segreta, Calcolo di MAC, Cifratura e Decifratura).

### 4.4.1 Message Digest per MAC

Un possibile schema di autenticazione a chiave segreta (composta da "sfide") è il seguente. Questo schema, purtroppo, presenta delle vulnerabilità...così come il seguente: Le vulnerabilità degli algoritmi di digest MD, sono note e facilmente attuabili in un possibile attacco. Infatti, MD(m) è calcolabile da tutti coloro che conoscono m e l'algoritmo di digest MD senza conoscere la chiave segreta!! Poiché, dall'input m si ottiene un messaggio mp avente lunghezza pari ad un multiplo intero di 512 bit (mediante un opportuno padding che include, tra l'altro, la lunghezza originaria di m), mp viene decomposto in chunk (pezzi) da 512 bit il digest viene ottenuto mediante una procedura iterativa, quindi il digest all'n-esima iterazione dipende esclusivamente dall'n-esimo chunk e dal digest ottenuto all'(n - 1)-esima iterazione...il digest risultante di m è il digest ottenuto all'ultima iterazione. Se un attaccante intercetta  $\langle m, MD(K_{AB}|m) \rangle$  tra Alice e Bob, l'attaccante senza conoscere la chiave segreta  $K_{AB}$  può calcolare il MAC di  $\langle m^+, MD(K_{AB}|m^+) \rangle$  (dato che l'algoritmo di hash è noto) tramite l'ultimo messaggio intercettato.

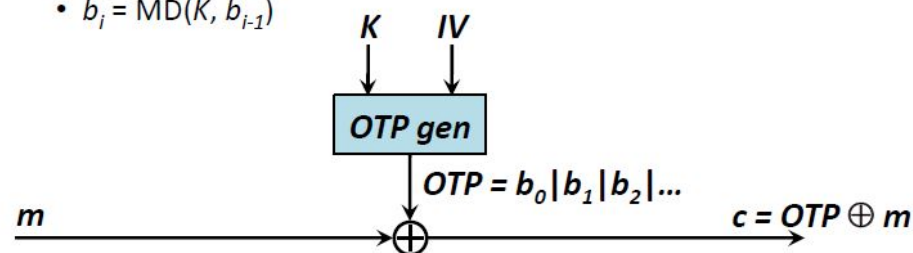
Una possibile soluzione è che il segreto  $K_{AB}$  sia messo in coda, a patto che l'algoritmo di hash sia molto resistente alle collisioni!! Un'altra possibilità è quella di utilizzare come MAC un sot-



$$- OTP = OTP(K, IV) = b_0 | b_1 | b_2 | \dots | b_i | b_{i+1} | \dots$$

- dove

- $b_0 = MD(K, IV)$
- $b_1 = MD(K, b_0)$
- ...
- $b_i = MD(K, b_{i-1})$



toinsieme arbitrario del digest MD, in questo caso, se il mio MAC è di soli 64 bit (invece di 128), l'attaccante potrebbe sempre ricostruire un messaggio da accodare...ma ha una possibilità su  $2^{64}$  che il MAC ottenuto sia quello corretto.

Una terza soluzione è quella di inserire il segreto  $K_{AB}$  sia all'inizio che in coda del messaggio da mandare al digest MD, così che  $K_{AB}$  in testa fornisca resistenza alle collisioni e  $K_{AB}$  rende innocua la vulnerabilità insita negli algoritmi di hash. Dato che ognuna delle soluzioni è equivalentemente corretta per ovviare al problema della vulnerabilità della funzione MD, per dare una piattaforma condivisa...una soluzione condivisibile da tutti, è stato introdotto il framework **HMAC** (keyed-Hash Message Authentication Code); l'algoritmo HMAC calcola due volte il digest del messaggio, e ogni volta inserisce in testa il segreto  $K_{AB}$ .

#### 4.4.2 Cifratura/Decifratura

Come faccio a cifrare con un algoritmo di hash? Devo utilizzare la funzione di hash potendo rendere tutto il processo invertibile, quindi introducendo lo XOR tra un chunk del messaggio e l'hash della chiave (genero un keypad) e ottengo un cifrario a flusso!!

#### 4.4.3 Algoritmi di cifratura come algoritmi di hash

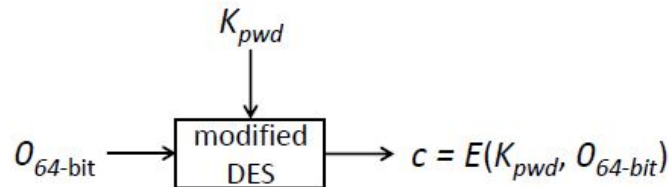
Se un algoritmo di hash/digest, può essere utilizzato come un algoritmo di cifratura...può accadere il contrario? In genere, questo principio è utilizzato (ad esempio) per la memorizzazione degli hash delle password in UNIX. Ma come si modifica un algoritmo di cifratura che sia resistente alle collisioni?

Lo schema di funzionamento (minimale) è questa Ma questo schema funziona per soli messaggi

**Fase 1**  $pwd \rightarrow K_{pwd}$

a partire dalla password  $pwd$  viene calcolata una chiave segreta  $K_{pwd}$

**Fase 2**



corti e non è troppo resistente alle collisioni, sebbene  $K_{PWD}$  sia ottenuta dalla  $pwd$  considerando i primi 8 caratteri ed espansa con i bit di parità per ogni gruppo di 8 bit. Dato  $s$  il *salt*, ovvero il numero di 12 bit ottenuto in modo pseudo randomico dalla  $pwd$  di ogni utente, la funzione  $h(pwd)$  si ottiene dal DES modificato che dipende dal valore di  $s$  (che determina quali bit devono essere replicati nella fase di espansione di  $R$  da 32 a 48 bit). Infine il DES modificato è utilizzato con  $K_{PWD}$  per cifrare una costante 0 a 64 bit. Il risultato della cifratura e il *salt*, sono memorizzati per poter recuperare  $pwd$ .

#### 4.4.4 Hash di grandi messaggi con algoritmi di cifratura come hash

Per l'algoritmo precedente, era stato sottolineato che era valido esclusivamente per messaggi corti. Come si deve operare per estendere questi algoritmi a messaggi di lunghezza arbitraria? Si può pensare di suddividere il messaggio  $m = m_1, m_2, m_3, \dots, m_n$ , ogni  $m_i$  viene utilizzato come input a un blocco in cascata di cifratura, alla fine della cascata ho realizzato un algoritmo di hash tramite cifratura...per un messaggio di lunghezza qualsiasi.

Purtroppo questo sistema soffre degli stessi problemi di cui soffriva il DES doppio, per ovviare ciò, basta rendere l'output di ogni blocco differente diverso dall'input del successivo, una possibile implementazione è la seguente

#### 4.4.5 Rainbow Tables (Opzionale)

Le Rainbow tables sono un meccanismo per l'attacco di reverse hash. Le tables bilanciano memoria e sforzo computazionale, se fosse utilizzata solo memoria si avrebbero dei database troppo grandi per poter mappare tutte le immagini degli hash e se fosse utilizzata solo potenza computazionale servirebbe troppo tempo per poter trovare l'inverso di un hash.

Le Rainbow tables utilizzano delle funzioni di riduzione  $r()$ , la funzione di riduzione è una applicazione dallo spazio degli Hash allo spazio dei Plaintext,  $r()$  non è l'inversa di un algoritmo di hash; per questo, prima di avvicinarmi a una buona inversione dovrò concatenare fino a centinaia di iterazioni di  $h(m) = k \rightarrow r(k) = m'$ . Per popolare la table, si memorizzano solo il messaggio iniziale e il messaggio finale della catena. In questo modo, con una catena di 100 iterazioni (dato che le funzioni sono deterministiche) si risparmia uno spazio in memoria di 100 volte la grandezza della table, in confronto a memorizzare solo coppie  $\langle plaintext, hash \rangle$ . Per recuperare un plaintext di un hash, si controlla se questo sia un endpoint di una qualsiasi delle catene (fase di lookup), se non lo fosse si controllano gli endpoint intermedi di ogni catena. Appena recuperato l'hash giusto, si utilizza la catena determinata dall'inizio finché non si trova l'hash di inizio; il messaggio che ha generato quell'hash sarà ciò che si cercava.

