Crittografia – Cenni

Damiano Carra

Università degli Studi di Verona
Dipartimento di Informatica

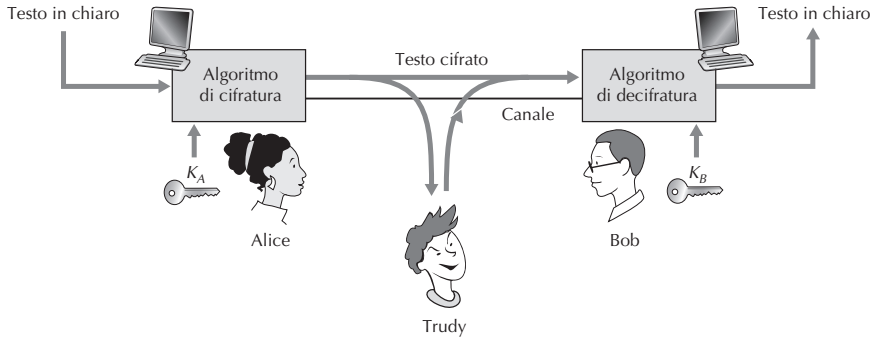
La crittografia

- Scienza che si occupa di proteggere l'informazione rendendola sicura, in modo che un utente non autorizzato che ne entri in possesso non sia in grado di comprenderla

- La crittoanalisi è invece la scienza che cerca di aggirare o superare le protezioni crittografiche, accedendo alle informazioni protette
  - L'insieme di crittografia e crittoanalisi è detto crittologia

Elementi del processo crittografico

- Algoritmo crittografico
  - Funzione che prende in ingresso un messaggio e un parametro detto chiave, e produce in uscita un messaggio trasformato
  - Cifratura
    - Testo in chiaro (plaintext o cleartext) → Testo cifrato (ciphertext)
  - Decifratura
    - Testo cifrato → Testo in chiaro



Elementi del processo crittografico

- Se le chiavi di cifratura e decifratura sono uguali
  - Algoritmo simmetrico
  - La chiave deve essere segreta
- Se le chiavi sono diverse
  - Algoritmo asimmetrico
  - Una chiave è pubblica, l'altra privata (segreta)

Robustezza crittografica

- Non deve essere possibile (facilmente...):
  - Dato un testo cifrato ottenere il corrispondente testo in chiaro senza conoscere la chiave di decifratura
  - Dato un testo cifrato e il corrispondente testo in chiaro ottenere la chiave di decifratura
- In generale, nessun algoritmo crittografico è assolutamente sicuro, quindi si dice che è computazionalmente sicuro se:
  - il costo necessario a violarlo è superiore al valore dell'informazione cifrata
  - il tempo necessario a violarlo è superiore al tempo di vita utile dell'informazione cifrata

Crittoanalisi

- La crittoanalisi tenta di ricostruire il testo in chiaro senza conoscere la chiave di decifratura
- L'attacco più banale è quello "a forza bruta"
  - Tentare di decifrare il messaggio provando tutte le chiavi possibili.
  - Applicabile a qualunque algoritmo, ma la sua praticabilità dipende dal numero di chiavi possibili.
  - È comunque necessario avere informazioni sul formato del testo in chiaro, per riconoscerlo quando si trova la chiave giusta.
- Principio di Kerckhoffs
  - Nel valutare la sicurezza di un algoritmo crittografico si assume che il crittoanalista conosca tutti i dettagli dell'algoritmo
  - La segretezza deve risiedere nella chiave, non nell'algoritmo!

Crittografia a chiave simmetrica

- La crittografia simmetrica, altrimenti detta crittografia a chiave segreta, utilizza una chiave comune e il medesimo algoritmo crittografico per la codifica e la decodifica dei messaggi
- Due utenti che desiderano comunicare devono accordarsi su di un algoritmo e su di una chiave comuni
  - La chiave deve essere scambiata su un canale sicuro

Cifrario di Cesare

- Sostituisce ogni lettera del testo in chiaro con quella che si trova K posizioni più avanti nell'alfabeto
  - K è la chiave
- Esempio: K = 3
  - In chiaro: A B C D E F G H I L M N O P Q R S T U V Z
  - Cifrate: D E F G H I L M N O P Q R S T U V Z A B C
  - Esempio di messaggio in chiaro / cifrato: CIAO / FNDR
- Le chiavi possibili sono solamente 20

Cifratura monoalfabetica

- Ogni carattere viene sostituito da un altro (permutazione), secondo un certo alfabeto che costituisce la chiave
- Esempio:
  - In chiaro: A B C D E F G H I L M N O P Q R S T U V Z
  - Cifrate: M Z N C B V L A H S G D F Q P E O R I T U
  - Esempio di messaggio in chiaro / cifrato: CIAO / NHMF
- Le chiavi possibili sono pari al numero di permutazioni possibili
  - 21! ovvero circa $5{,}1 \times 10^{19}$

Analisi delle frequenze

- Spazio delle chiavi di un algoritmo monoalfabetico molto grande
  - Ma la crittoanalisi è semplice tramite l'analisi delle frequenze
- In un testo scritto in una determinata lingua (italiano, inglese...) ogni lettera dell'alfabeto si presenta secondo una certa frequenza:
  - Ad esempio in italiano E ed A sono molto comuni, Q e Z sono poco comuni
  - E poi ci sono gruppi di 2 o 3 lettere ("ch", "che", "qu", …)
- Contando il numero di occorrenze di ogni lettera nel testo cifrato è possibile ipotizzare con buona probabilità quale sia la lettera corrispondente

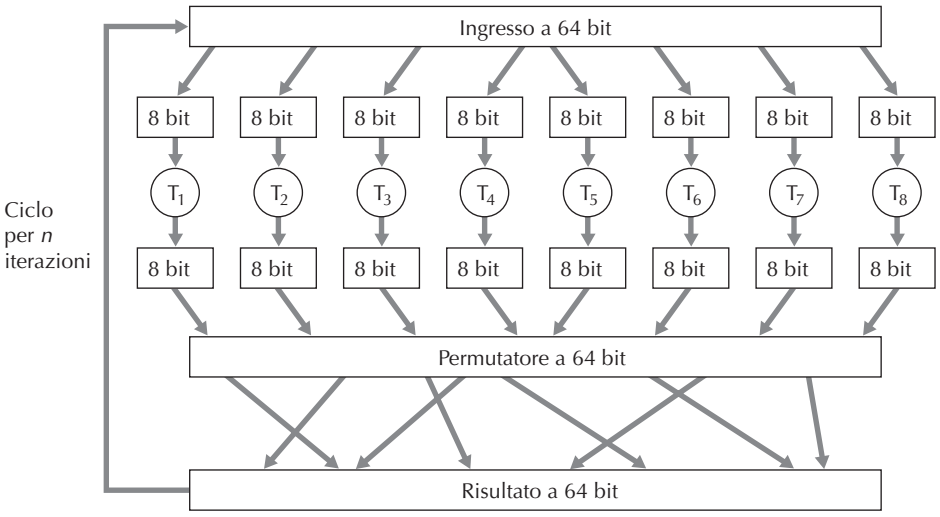
Cifrari a blocchi

- Tecniche di cifratura simmetrica
  - Usati in molti protocolli sicuri di Internet, compreso PGP (posta elettronica), SSL (connessione TCP) e IPSec (trasmissione a livello di rete)
  - Chiamati anche cifrari a flusso
- Dati k bit, i possibili 2^k ingressi vengono permutati
- Esempio: k = 3

Ingresso	Uscita	Ingresso	Uscita
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

Cifrari a blocchi (cont'd)

- Le permutazioni possono essere combinate tra loro per creare schemi più complessi



Esempi

- DES (Data Encryption Standard)
  - È il più noto algoritmo crittografico simmetrico moderno, Nato negli anni ‘70 a seguito di un progetto di IBM
  - Adottato ufficialmente nel ‘77 come standard dal governo americano
  - Utilizza chiavi di 56 bit → da considerarsi ormai obsoleto
- Triplo-DES
  - Per aumentare la sicurezza del DES lo si applica tre volte con chiavi diverse
  - Esistono due varianti
    - con chiave da 112 bit (56 × 2)
    - con chiave da 168 bit (56 × 3)

AES - Rijndael

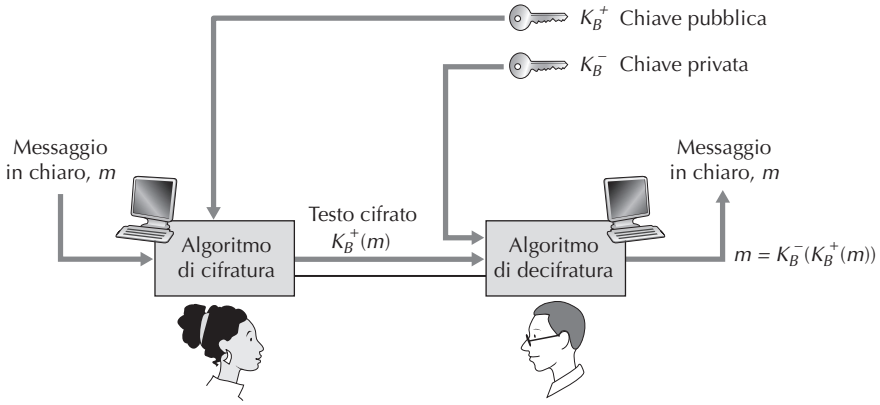
- Nel 1997 il NIST (National Institute of Standards and Technology) ha bandito una gara per trovare il successore del DES come algoritmo standard
  - AES: Advanced Encryption Standard
- Nell’ottobre 2000 è stato scelto come vincitore l’algoritmo Rijndael, sviluppato da due crittologi belgi
  - Joan Daemen e Vincent Rijmen
- AES è un algoritmo simmetrico che può utilizzare chiavi di 128, 192 o 256 bit (AES-128, AES-192, AES-256).
- AES sta gradualmente soppiantando il triplo DES.

Distribuzione delle chiavi

- Negli algoritmi simmetrici la chiave è la stessa in cifratura e decifratura
  - Dunque deve essere segreta
- Esiste quindi il problema della distribuzione delle chiavi
  - Serve un canale di comunicazione sicuro per trasmettere la chiave
- Nel 1976 Diffie e Hellman propongono uno schema che supera questa limitazione
  - Crittografia a chiave pubblica (o asimmetrica)

Chiave pubblica / chiave privata

- Nella crittografia asimmetrica ogni utente ha una coppia di chiavi, costituita da una chiave pubblica e una chiave privata
  - La chiave pubblica viene resa nota, quella privata deve rimanere segreta
- Il dato viene cifrato con la chiave pubblica del destinatario, che potrà decifrarlo con la propria chiave privata



Crittografia asimmetrica

- Vantaggi:
  - Non è più necessario incontrarsi per scambiare chiavi.
  - La stessa chiave (pubblica) può essere usata da più utenti.
- Requisiti:
  - Deve essere semplice la generazione di una coppia di chiavi pubblica/ privata
  - Deve essere semplice l'operazione di cifratura e decifratura se si è a conoscenza della relativa chiave
  - Deve essere computazionalmente impraticabile ricavare la chiave privata da quella pubblica
  - Deve essere computazionalmente impraticabile ricavare il testo in chiaro avendo il testo cifrato e la chiave pubblica

Algoritmo RSA

- RSA (1977), così chiamato dalle iniziali dei suoi inventori (Rivest, Shamir, Adleman), è sicuramente il più noto algoritmo crittografico asimmetrico
- Si basa sulla difficoltà di ***scomporre un numero in fattori primi***
- La chiave in RSA ha di solito dimensioni di almeno 2^{10} bit
  - Oltre 300 cifre decimali
- Un attacco a forza bruta contro RSA non consiste nel provare tutte le chiavi possibili, ma nel fattorizzare il prodotto di due numeri primi

Algoritmo RSA (cont'd)

- Per capire come avviene la cifratura e la decifratura con RSA ci si deve avvalere della matematica a modulo
- Scelti due primi p,q si calcola
  - $n = p*q$
  - $z = (p-1)*(q-1)$
  - un numero $1 < e < n$ relativamente primo a z
  - un numero d tale che $(e*d-1)$ sia multiplo di z
- Chiave pubblica → (n,e) Per cifrare m → $c = m^e \bmod n$
- Chiave privata → (n,d) Per decifrare c → $m = c^d \bmod n$

Algoritmo RSA: esempio

- p = 5, q = 7
- Segue:
  - n = p*q = 35
  - z = (p-1)*(q-1) = 24
  - e = 5 (relativamente primo a 24; andavano bene anche 7, 9, 11, …)
  - d = 29 (infatti 5*29 – 1 = 144 → multiplo di 24)
- Messaggio da inviare: la parola "love"
  - Supponiamo di rappresentare le lettere con numeri da 1 a 26 (incluse le lettere x,y,w, …)

Algoritmo RSA: esempio

Lettere in chiaro	m: rappresentazione numerica	m^e	Testo cifrato $c = m^e \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Testo cifrato c	c^d	$m = c^d \bmod n$	Lettere in chiaro
17	481968572106750915091411825223071697	12	l
15	12783403948858939111232757568359375	15	o
22	851643319086537701956194499721106030592	22	v
10	10000000000000000000000000000000	5	e

Algoritmi asimmetrici: considerazioni

- Richiedono molte risorse computazionali
  - 100-1000 volte più lenti degli algoritmi simmetrici
- Vengono utilizzati per scambiarsi una chiave di sessione
  - La chiave di sessione verrà poi usata con un algoritmo simmetrico sicuro e computazionalmente più efficiente
- Con RSA ciò che viene cifrato con la chiave pubblica si può decifrare con la chiave privata...
- ...ma vale anche l'inverso: ciò che è cifrato con la chiave privata si può decifrare con la chiave pubblica!
- Questo fornisce un mezzo per garantire l'autenticazione
  - Argomento della prossima lezione