Sabrina De Capitani di Vimercati

decapita@ing.unibs.it.

DEA - Università di Brescia

Scopo delle Lezioni

- metodi crittografici moderni
  - a chiave simmetrica
  - a chiave asimmetrica
- loro applicazione alla sicurezza della trasmissione digitale
  - reti

Cosa è la Crittografia?

È una disciplina che si occupa della protezione dei dati

- Tradizionalmente, la crittografia viene vista come una tecnica per preservare la segretezza (confidentiality) della informazione
- La segretezza è solo uno degli aspetti trattati dalla crittografia moderna

Applicazioni nella Sicurezza delle Trasmissioni

- Confidenzialità/segretezza
- Integrità
- Autenticità/non-ripudio
- Firma digitale
- Diritto d’autore

Scenario

Good Guys...

- Alice vuole comunicare con Bob usando un canale di comunicazione insicuro

...and Bad Guys

- Eva vuole “ascoltare” la comunicazione lungo questo canale di comunicazione e:
  - carpire i messaggi tra Alice e Bob
  - alterare il contenuto di questi messaggi

Terminologia (1)

Crittografia:

arte che si occupa della protezione delle informazioni

Cifratura o crittazione (encryption):

operazione tramite la quale si proteggono le informazioni; usa una chiave

Cifrario (cipher):

algoritmo tramite il quale viene effettuata la cifratura

Testo in chiaro (plaintext):

messaggio da cifrare (proteggere)

Testo cifrato o crittogramma (ciphertext):

output del processo di cifratura

Terminologia (2)

Decifratura o decrittazione (decryption):

trasformazione del testo cifrato in testo in chiaro; usa una chiave

Crittosistema:

ambito nel quale sono effettuate le operazioni di crittazione e decrittazione

Crittoanalisi:

pratica del rivelare ciò che la crittografia tenta di proteggere

Crittologia:

include sia la crittografia che la crittoanalisi

Principio di Kerckhoff

Il crittanalista sa sempre quale crittosistema è stato usato e ne conosce gli algoritmi

Solo la chiave è segreta

Scenari Crittoanalitici

- Ciphertext only: noto solo il crittotesto
- Known plaintext: testo in chiaro noto
- Chosen plaintext: testo in chiaro scelto
- Brute force attack: attacco alla chiave

Un pò di Storia

La crittografia ha una lunga storia.....
Il libro di Geremia nella Bibbia usa un codice monoalfabetico (il cifrario di Atbash) per cifrare la parola Babele

Alfabeto Ebraico

Alef (prima lettera)	$\rightarrow$	Taw (ultima lettera)
Beth (seconda lettera)	$\rightarrow$	Shin (penultima lettera)
Ghimel (terza lettera)	$\rightarrow$	Sin (terzultima lettera)
...	...	...

Classificazione Metodi di Cifratura

- Cifrari a sostituzione: operano sostituendo alle lettere del messaggio in chiaro una o più lettere dell'alfabeto in accordo ad uno schema prefissato (chiave segreta)
  - monoalfabetici: ad ogni lettera del messaggio in chiaro corrisponde una unica lettera del crittogramma
  - polialfabetici: ad ogni lettera del messaggio in chiaro corrisponde una lettera scelta in un *insieme di lettere possibili*
- Cifrari a trasposizione: permutano le lettere del messaggio in chiaro in accordo ad una funzione di trasposizione fissata (chiave segreta)

Monoalfabetico - La Scacchiera di Polibio

Polibio storico greco, 200–118 a.C.

- ogni lettera è cifrata da una coppia di numeri compresi tra 1 e 5 in base ad una scacchiera 5x5
- più che un codice segreto è un sistema di telecomunicazione ottico
- La sua importanza sta nel fatto che è alla base di altri codici di cifratura quali, ad esempio, il Playfair Cipher

Esempio di Cifratura con la Scacchiera di Polibio

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	kq	l	m	n	o
4	p	r	s	t	u
5	v	w	x	y	z

Attenzione agli attacchi $\rightarrow$ 11 44 44 15 34 55 24 35 34 15 11 22 32 24 11 44 44 11 13 13 23 24

Cifrari Affini

La lettera a_i viene sostituita con la lettera

$$a_{k \cdot i + h} \; mod \; 26$$

La chiave è la coppia (k, h) con:

$$k, h \in \{0, 1, \ldots, 25\}$$

MCD(k,26) = 1

Porre MCD(k,26) = 1 serve per garantire che la funzione che fa corrispondere ad i il valore $k \cdot i + h$ sia una corrispondenza biunivoca

Cifrari Affini - Attacco alla Chiave

Quante chiavi ha un crifario affine?

k dispari e k $\neq$ 13 $\rightarrow$ 12 valori di k

h può assumere 26 valori

12 x 26 = 312 chiavi diverse

Un attacco di forza bruta deve in media provare 156 chiavi!

Si osservi che la chiave (1,0) corrisponde alla sostituzione identica

Cifrari Affini - Attacco alle Frequenze

Sia $f(x)$ la frequenza della lettera x nel crittogramma e supponiamo che:

- G e N siano le lettere più frequenti con $f(G) > f(N)$
- la lingua è l'italiano

$\Rightarrow$ G e N corrispondono rispettivamente ad E ed A nel testo in chiaro

pos(G) = k · pos(E) + h 6 = 4k + h (mod 21)
pos(N) = k · pos(A) + h 11 = 0k + h (mod 21)

La chiave è: (4,11)

Polialfabetico - Playfair (1)

Inventato dal fisico sir Charles Wheatstone (1802–1875) e diffuso nelle sfere governative da Lyon Playfair

c	o	m	p	u
t	e	r	a	b
d	f	g	h	i
j	k	l	n	q
s	v	x	y	z

Il messaggio da cifrare viene suddiviso in bigrammi di due lettere consecutive sostituite in accordo alle seguenti regole

Polialfabetico - Playfair (2)

- lettere sulla stessa riga $\rightarrow$ due lettere che le seguono a destra (ciclico)
- lettera sulla stessa colonna $\rightarrow$ due lettere sottostanti (ciclico)
- lettere in colonne e linee diverse $\rightarrow$ si prendono le lettere che costituiscono un rettangolo con esse
- se il bigramma presenta due lettere uguali si cerca di eliminare il raddoppio oppure di romperlo inserendo una lettera rara (k, w, x, y)

Esempio di Cifratura con il Playfair Cipher

c	o	m	p	u
t	e	r	a	b
d	f	g	h	i
j	k	l	n	q
s	v	x	y	z

Messaggio in chiaro: INVIARE SUBITO NUOVE TRUPPE
Divisione in bigrammi: IN VI AR ES UB IT ON UO VE TR UP YP E
Messaggio cifrato: HQ FZ BA TV BI BD PK CM OF EA CU PA E

Cifrari a Trasposizione

Effettuano una permutazione delle lettere che compongono il messaggio

- il messaggio viene permutato lettera per lettera
- singolo passo di trasposizione; altri adottano due passi di trasposizione
- molti si basano su figure geometriche
- metodi di trasposizione a “griglia”

Esempio di Trasposizione Colonnare

Si fissa la larghezza della matrice ed il messaggio viene inserito per righe ed estratto per colonne

p: enemy tanks approaching hill eight six three

e	n	e	m	y	t	a
n	k	s	a	p	p	r
o	a	c	h	i	n	g
h	i	l	l	e	i	g
h	t	s	i	x	t	h
r	e	e				

c: ENOHHRNKAITEESCLSEMAHLIYPIEXTPNITARGGH

Esempio di Trasposizione a Percorso: Rail-Fence

p: reinforcements arriving now

			N						M						R						G			
		I		F				E		E				A		R				N		N		
	E				O		C				N		S				I		I				O	
R						R						T						V						W

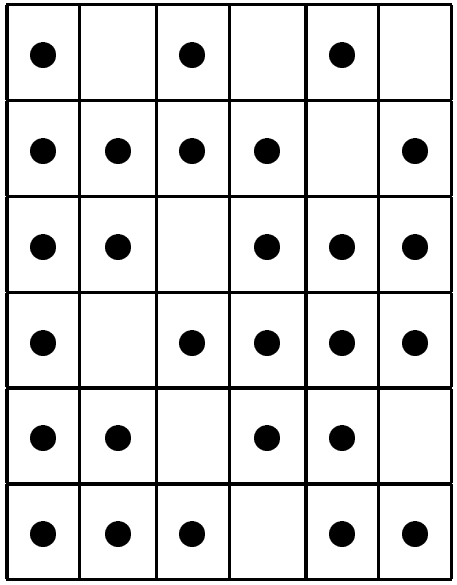
c: NMRGIFEEARNNEOCNSIIORRTVW

Cifrario a Griglia

- matrice 6x6 nella quale alcune caselle sono piene ed altre sono vuote
- il messaggio viene scomposto in blocchi di lunghezza 36
- le prime 9 lettere del blocco vengono inserite in una matrice 6x6 (nelle caselle bianche della griglia)
- si ruota la griglia di 90 gradi in senso orario e si ripete il procedimento (il tutto deve essere ripetuto 4 volte)

Esempio Cifrario a Griglia (1)

Schema della griglia: 9 celle sono scoperte mentre le restanti 27 sono coperte (●)



Esempio Cifrario a Griglia (2)

p: non sono io colpevole ma è il tuo amico carlo

•	N	•	O	•	N
•	•	•	•	S	•
•	•	O	•	•	•
•	N	•	•	O	•
•	•	•	•	•	I
•	•	•	O	•	•

Passo 1

•	•	•	•	•	•
•	•	C	•	•	O
•	•	•	L	•	•
P	•	•	•	•	E
•	•	V	•	O	•
•	L	•	•	•	E

Passo 2

Esempio Cifrario a Griglia (3)

•	•	M	•	•	•
A	•	•	•	•	•
•	E	•	•	I	•
•	•	•	L	•	•
•	T	•	•	•	•
U	•	O	•	A	•

Passo 3

M	•	•	•	I	•
•	C	•	O	•	•
C	•	•	•	•	A
•	•	R	•	•	•
L	•	•	O	•	•
•	•	•	•	•	•

Passo 4

Esempio Cifrario a Griglia (4)

M	N	M	O	I	N
A	C	C	O	S	O
C	E	O	L	I	A
P	N	R	L	O	E
L	T	V	O	O	I
U	L	O	O	A	E

Cifrari Sicuri: One-time Pad

- Proposto da Vernam e Mauborgne nel 1917
- Usato per le comunicazioni segrete tra Washington e Mosca durante la guerra fredda
- Per usare questo cifrario si deve assumere che i messaggi e le chiavi siano *sequenze di bit*
- Le trasformazioni da *M* a *C* e viceversa sono basate sulla funzione matematica XOR

		XOR
0	0	0
0	1	1
1	0	1
1	1	0

Cifratura/Decifratura con One-Time Pad

$M = m_1 m_2 \ldots m_n$ (lunghezza n)
$K = k_1 k_2 \ldots k_n$ è una chiave dove ogni bit k_i è scelto perfettamente a caso e che viene comunicata al destinatario di M (lunghezza n)

Cifratura

- $C = c_1 c_2 \ldots c_n$ dove $c_i = m_i \oplus k_i, i = 1, \ldots, n$

Decifratura

- $M = c_i \oplus k_i, i = 1, \ldots, n$

Metriche

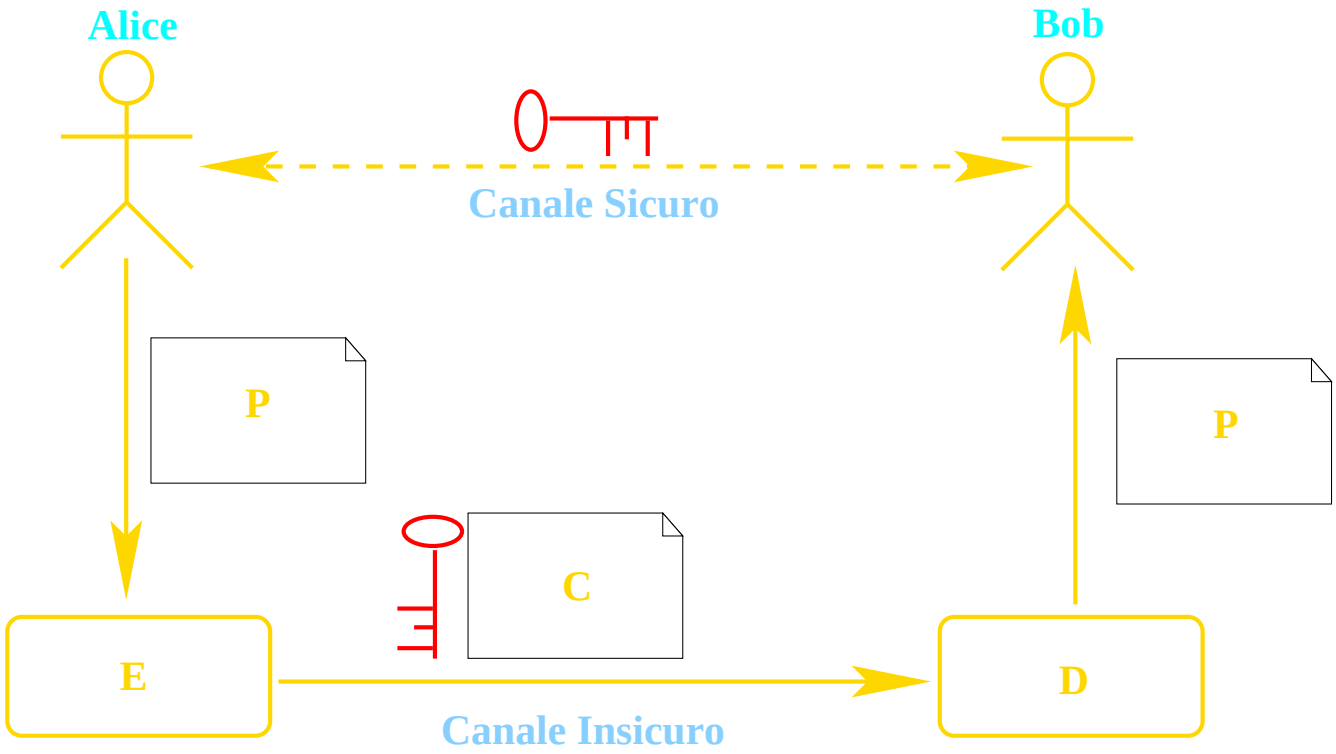
- Incondizionato sicuro: dato un qualsiasi crittogramma è impossibile risalire al corrispondente messaggio in chiaro anche se si dispone di “risorse infinite”
  $\Rightarrow$ One-Time Pad è incondizionato sicuro
- Computazionalmente sicuro: è *difficile in pratica* risalire al messaggio in chiaro sebbene il corrispondente crittogramma contiene abbastanza informazione per risalire al messaggio in chiaro usando un grande quantità di risorse

Computazionalmente Sicuro

- Da questo momento in poi considereremo crittosistemi che sono computazionalmente sicuri
- Questi crittosistemi sono basati su problemi difficili quali la fattorizzazione di interi, il calcolo del logaritmo discreto
  - Problemi facili: trovare il valore massimo tra n numeri (O(n)) oppure ordinare n elementi (O($n \log n$))
  - Problemi difficili: fattorizzare N (numero lungo n bit) ($2^{O(\sqrt{n \cdot \log n})}$)

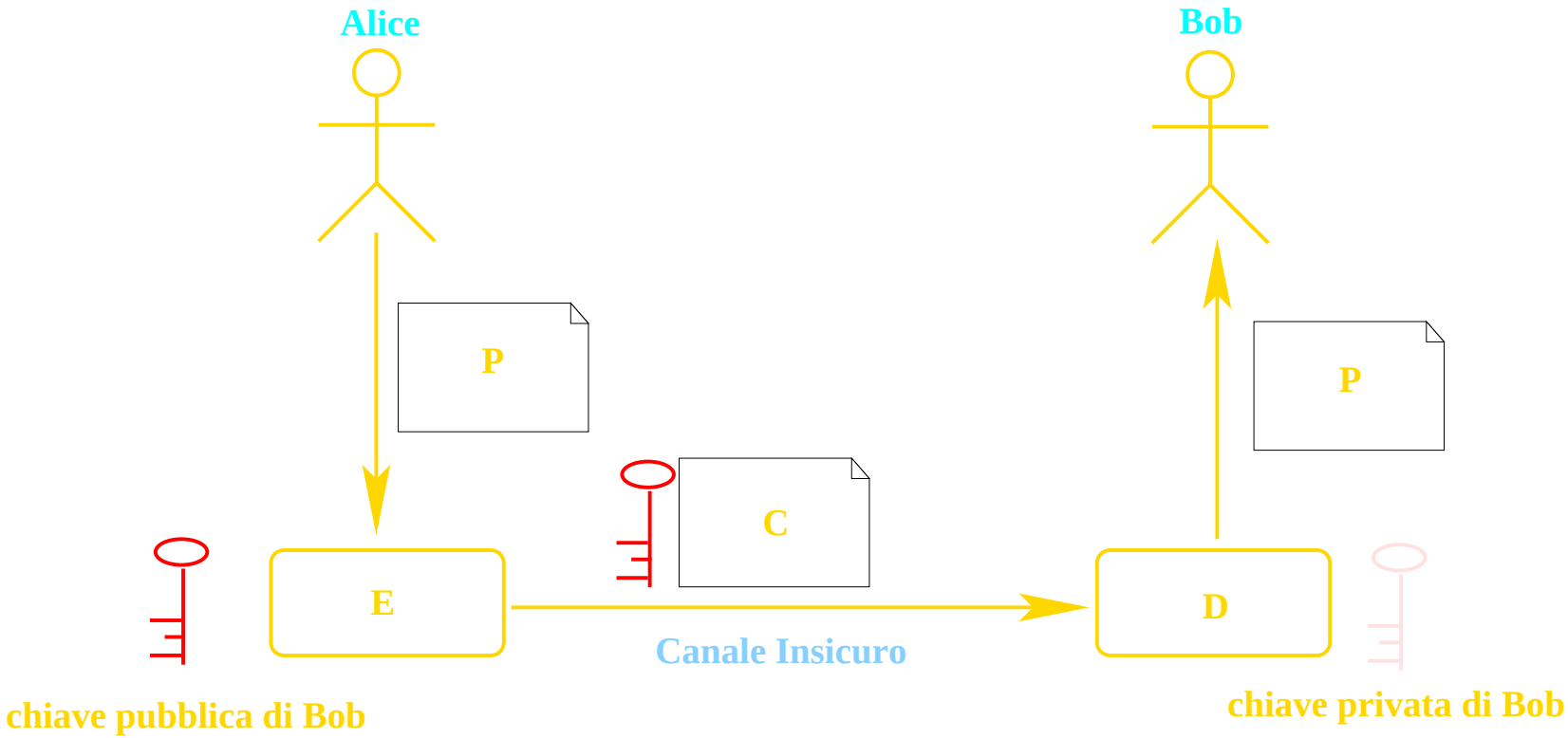
Crittosistemi a Chiave Simmetrica

Sono anche chiamati crittosistemi a chiave segreta



Crittosistemi a Chiave Asimmetrica

Sono anche chiamati crittosistemi a chiave pubblica



Prima Osservazione: Numero di chiavi

Simmetrici:
per n utenti che comunicano a due a due:

$$\frac{n(n-1)}{2}$$

Asimmetrici:
per n utenti che comunicano in qualsiasi modo:

$$2n$$

di cui n pubbliche ed n private

....la prossima volta DES

