

Crittografia 1 - CR410

Francesca Merola

informazioni

- orario:
martedì 11:00-13:00 aula F
mercoledì 16:00-18:00 aula G
venerdì 11:00-13:00 aula F (più o meno a settimane alterne)
- ricevimento: su appuntamento email
(martedì pomeriggio ?) studio 300
- pagina web:
<http://ricerca.mat.uniroma3.it/users/merola/>
- email: merola@mat.uniroma3.it

Testi consigliati

- Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici
- D. Stinson: Cryptography - theory and practice
- Languasco, Zaccagnini: Manuale di crittografia
- Katz, Lindell: An introduction to modern cryptography
- B. Schneier: Applied Cryptography

schema del corso

- Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici. Introduzione alla crittoanalisi.
- Introduzione alla crittografia a chiave pubblica. Cenni di teoria della complessità. Problema dello zaino. Cifrario di Merkle-Hellman.
- Il crittosistema RSA. Test di primalità. Algoritmi di fattorizzazione. Alcuni attacchi all'RSA. Cifrario di Rabin.
- Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal.
- Firma digitale. Schemi di firma. Lo schema RSA. Lo schema di Elgamal. Cenni su alcuni protocolli crittografici.

crittografia

Crittografia - dal greco

κρυπτος, nascosto

γραφειν, scrivere

crittografia

crittologia

crittoanalisi

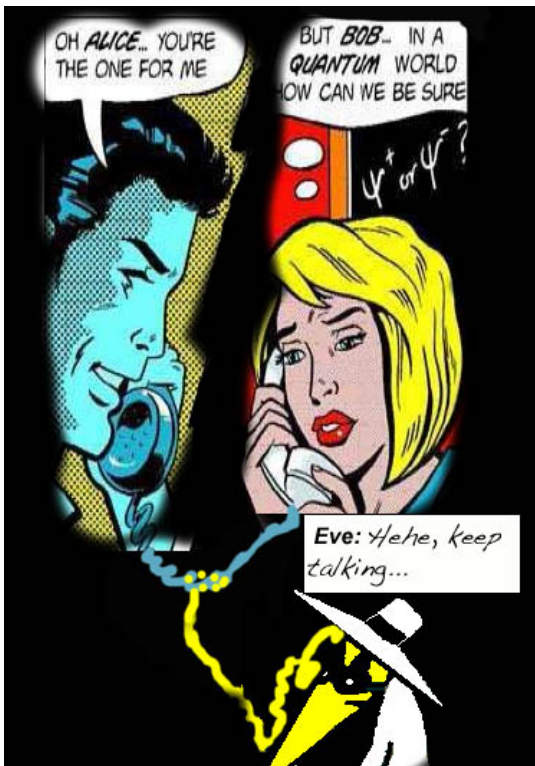
- classicamente, crittografia = nascondere il contenuto di un messaggio
- più di recente, molti altri usi:
 - autenticazione di un messaggio/interlocutore
 - scambio di una chiave segreta
 - firma digitale
 - condivisione di un segreto
 - e molto altro



Alice



Bob



Alice



Bob

← Eve

atbash - un cifrario a sostituzione



Hebrew scribes used the reverse-alphabet *Atbash* cipher. Names of people and places are believed to have been deliberately obscured in the Hebrew Bible using this code. It substitutes the first letter of the alphabet for the last and the second letter for the second last, and so on.

ABCDEFGHIJKLM

ZXYWVUTSRQPON

ciao → YRZL

la scitola - un cifrario a trasposizione



crittosistema: definizione

Definizione

Un crittosistema è una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, dove

- ① \mathcal{P} è un insieme finito di testi in chiaro (plaintext)
- ② \mathcal{C} è un insieme finito di testi cifrati (ciphertext)
- ③ \mathcal{K} è un insieme finito di chiavi. (\mathcal{K} è detto spazio delle chiavi)
- ④ per ogni $k \in \mathcal{K}$ c'è una funzione di cifratura $e_k \in \mathcal{E}$,
 $e_k : \mathcal{P} \rightarrow \mathcal{C}$ e una funzione di decifratura $d_k \in \mathcal{D}$, $d_k : \mathcal{C} \rightarrow \mathcal{P}$
tali che, per ogni $x \in \mathcal{P}$ si ha

$$d_k(e_k(x)) = x$$

se si ha $x, y \in \mathcal{P}$ con $x \neq y$,
allora dev'essere anche, per ogni chiave k , $e_k(x) \neq e_k(y)$;
le funzioni di cifratura devono essere **iniettive**.

cifrario additivo (shift cipher)

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$;
- fissiamo $0 \leq k \leq 25$; allora
 - $e_k(x) = (x + k) \bmod 26$,
 - $d_k(y) = (y - k) \bmod 26$.

Nota: quando $k = 3$, si ha il [cifrario di Cesare](#).

Identifichiamo \mathbb{Z}_{26} con l'alfabeto:

A	B	C	D	E	F	G	H	I
0	1	2	3	4	5	6	7	8
J	K	L	M	N	O	P	Q	R
9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z	
18	19	20	21	22	23	24	25	

esempio

la chiave è $k = 9$

s	a	l	u	t	i	d	a	l	m	a	r	e
18	0	11	20	19	8	3	0	11	12	0	17	4
1	9	20	3	2	17	12	9	20	21	9	0	13
B	J	U	D	C	R	M	J	U	V	J	A	N

Nota: spesso si pensa la chiave come una lettera, non come un numero (in questo esempio la chiave è J).

Proprietà di un buon crittosistema:

- Dev'essere possibile calcolare ogni e_k e d_k in modo "efficiente";
- Eve non deve essere in grado di risalire al testo in chiaro (o peggio, alla chiave) dal testo cifrato.

Per i cifrari additivi, si hanno solamente 26 possibili chiavi!!

esercizio

Provare a **decrittare** il messaggio

L E E P Y E T L W N L Y P
a t t e n t i a l c a n e

la chiave è 11 (oppure L)

in un crittosistema, bisogna che
 $x, y \in \mathcal{P}, x \neq y, \Rightarrow e_k(x) \neq e_k(y)$; le funzioni di cifratura devono
essere iniettive.

\mathcal{P} e \mathcal{C} sono insiemi *finiti*

se in un crittosistema si ha $\mathcal{P} = \mathcal{C}$,

una funzione $f : \mathcal{P} \rightarrow \mathcal{C} = \mathcal{P}$

è iniettiva \Leftrightarrow è suriettiva \Leftrightarrow è biiettiva

dunque in questo caso le funzioni di cifratura sono

permutazioni di \mathcal{P}

permutazioni

Se X è un insieme finito con n elementi
un'applicazione **biiettiva** $\pi : X \rightarrow X$ si dice **permutazione** di X .

Ci sono $n! = n \cdot (n - 1) \dots 3 \cdot 2 \cdot 1$ permutazioni di X .

L'insieme delle permutazioni di un insieme con n elementi;
si denota con S_n .

cifrari a sostituzione

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$$

$$\mathcal{K} = \{ \text{permutazioni di } \mathbb{Z}_{26} \} = S_{26}$$

per ogni $\pi \in \mathcal{K}$, si ha

$$e_\pi(x) = \pi(x), \quad \text{e} \quad d_\pi(y) = \pi^{-1}(y).$$

identificheremo \mathbb{Z}_{26} con l'alfabeto

sia π la permutazione

a	b	c	d	e	f	g	h	i	j	k	l	m
F	X	H	G	N	O	K	A	U	P	S	V	T
n	o	p	q	r	s	t	u	v	w	x	y	z
Q	L	M	D	I	R	Y	C	J	E	Z	B	W

allora π^{-1} è

A	B	C	D	E	F	G	H	I	J	K	L	M
h	y	u	q	w	a	d	c	r	v	g	o	p
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
e	f	j	n	s	k	m	i	l	z	b	t	x

c i v e d i a m o p o i
 H U J N G U F T L M L U

Proprietà di un buon crittosistema:

- Dev'essere possibile calcolare ogni e_k e d_k in modo "efficiente";
- Eve non deve essere in grado di risalire alla chiave (o al testo in chiaro) dal testo cifrato.

Per i cifrari additivi, si hanno solamente 26 possibili chiavi!

Nel caso di una sostituzione generica, il numero di chiavi è molto alto

$$|\mathcal{K}| = 26! \approx 4 \cdot 10^{26}.$$

questo non basta a garantire la sicurezza!

cifrari a trasposizione

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$$

abbiamo una m -pla di lettere;

$$\mathcal{K} = \{ \text{permutazioni di } \{1, 2, \dots, m\} \} = S_m$$

per ogni $\pi \in \mathcal{K}$, $x = (x_1, x_2, \dots, x_m) \in \mathcal{P}$,

$y = (y_1, y_2, \dots, y_m) \in \mathcal{C}$ si ha

$$e_\pi(x) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)});$$

$$d_\pi(y) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)});$$

crittoanalisi: principio di Kerckhoffs

L'attaccante, Eve, può conoscere il crittosistema usato da Alice e Bob.

Non conosce la chiave.

Vantaggi:

- è più facile tenere segreta la chiave
- se la sicurezza si basa sulla chiave, e la chiave viene scoperta, basta cambiare chiave
- si può usare lo stesso crittosistema per far comunicare diverse coppie di persone

- oggi il principio di Kerckhoffs viene inteso in maniera più forte: l'algoritmo deve essere pubblico
- un sistema che viene molto studiato (e attaccato) è più sicuro
- meglio che le debolezze, se ci sono, vengano scoperte e rese pubbliche
- se l'algoritmo è pubblico, non c'è rischio di reverse engineering
- si possono stabilire standard

crittoanalisi: tipi di attacco

Ciphertext only attack: L'attaccante conosce una stringa y di testo cifrato. Cerca di risalire al testo in chiaro o alla chiave.

Known plaintext attack: L'attaccante conosce una stringa x di testo in chiaro e il corrispondente testo cifrato y . Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen plaintext attack: L'attaccante ha la possibilità di scegliere un testo in chiaro x e di ottenere il corrispondente testo cifrato. Cerca di risalire alla chiave o di decrittare altri testi cifrati.

Chosen ciphertext attack: L'attaccante ha la possibilità di scegliere un testo cifrato y e di ottenere il corrispondente testo in chiaro x . Cerca di risalire alla chiave.

crittoanalisi di un cifrario a sostituzione

Dobbiamo decrittare il testo

QANGH TGM YJ XGHTN AVUNG TTYSH LUXYU OUAUD UQQYJ UJAXX
YNUTY NGKGB BUGMA XASLG KJUGX YQANG HTGMY JXGHT DABBY
VUJAK TYTYT ANGHT JAKTY VUJHS SYOGH TSAOD JUQAD ABBYV
GQG XG SXGVU IHAJJ UQPAV UTMAN TYSUO AXXYT YTAJJ ASXHF
AATAU QGOUT AXXUD ANGQQ ATVAN AUJFH YQYAD ANNUS QGJVG
NAJAS XGTBA TYTSY QYOAG TVGSS AOGUJ FGXXY KJUAQ PAHTL
AJKUY NTYIH ASXYD ABBYV UJAKT YQGDU XYTAJ JGLYX XAKGV
UHTMA QQPUY FGJAK TGOAU JIHGJ AGMAM GTYOA OGSXN GTXYT
UYSAT YTQPA XHXXU JYQPU GOGMG TYOGA SXNYQ UJUAK UGDAN
MUGVA JJGDH TXGVA JSHYT GSYQP AANGS AODNA JHSXN GADGY
TGBBG QYOA H TGQUJ UAKUG OGXHN GGDDA TGOGA SXNYQ UJUAK
UGALL AMUSX YIHAJ DABBY VUJAK TYSUN GJJAK NYXHX XYAVG

analisi delle frequenze

frequenze dei caratteri % in italiano

A	B	C	D	E	F	G	H	I
10,41	0,95	4,28	3,82	12,62	0,75	2,01	1,10	11,62
J	K	L	M	N	O	P	Q	R
0	0	6,61	2,58	6,49	8,71	3,20	0,75	6,70
S	T	U	V	W	X	Y	Z	
6,04	6,06	3,04	1,51	0	0	0	0,93	

analisi delle frequenze

frequenze dei caratteri % nel nostro testo

A 13,52	B 2,41	C 0	D 2,78	E 0	F 0,74	G 11,30	H 4,26	I 0,74
J 6,85	K 2,59	L 1,11	M 1,85	N 4,44	O 2,96	P 1,11	Q 4,44	R 0
S 4,44	T 7,78	U 8,52	V 2,78	W 0	X 6,48	Y 8,89	Z 0	

proviamo A=e

QeNGH TGM YJ XGHTN eVUNG TTYSH LUXYU OUeUD UQQYJ UJeXX
 YNUTY NGKGB BUGMe XeSLG KJUGX YQeNG HTGMY JXGHT DeBBY
 VUJeK TYTYT eNGHT JeKTY VUJHS SYOGH TSeOD JUQeD eBBYV
 GQG XG SXGVU IHeJJ UQPeV UTM eN TYSUO eXXYT YTeJJ eSXHF
 eeTeU QGOUT eXXUD eNGQQ eTVeN eUJFH YQYeD eNNUS QGJVG
 NeJeS XGTBe TYTSY QYOeG TVGSS eOGUJ FGXXY KJUeQ PeHTL
 eJKUY NTYIH eSX YD eBBYV UJeKT YQGDU XYTeJ JGLYX XeKGV
 UHTMe QQPUY FGJeK TGOeU JIHGJ eGMeM GTY0e OGSXN GTXYT
 UYSeT YTQPe XHXXU JYQPU GOGMG TYOG e SXNYQ UJUeK UGDeN
 MUGVe JJGDH TXGVe JSHYT GSYQP eeNGS eODNe JHSXN GeDGY
 TGBBG QYOeH TGQUJ UeKUG OGXHN GGDe TGOG e SXNYQ UJUeK
 UGeLL eMUSX YIHeJ DeBBY VUJeK TYSUN GJJ eK NYXHX XYeVG

Digrammi frequenti in italiano (nell'ordine):

er, es, on, re, el, en, de, di, si, ti, la, al

Nel nostro testo:

AN (9), YT (9), AJ (6), VU (5).

(le nostre vocali sono probabilmente G, U, Y)

G=a, N=r, ?? Y=o, T=n, U=i ??.

QeraH naMoJ XaHnr eVira nnoSH LiXoi OieiD iQQoJ iJeXX
orino raKaB BiaMe XeSLa KJiaX oQera HnaMo JXaHn DeBBo
ViJeK nonon eraHn JeKno ViJHS SoOaH nSeOD JiQeD eBBoV
aQaXa SXaVi IHeJJ iQPeV inMer noSiO eXXon oneJJ eSXHF
eenei QaOin eXXiD eraQQ enVer eiJFH oQoeD erris QaJVa
reJeS XanBe nonSo QoOea nVaSS eOaiJ FaXXo KJieQ PeHnL
eJKio rnoIH eSXoD eBBoV iJeKn oQaDi XoneJ JaLoX XeKaV
iHnMe QQPio FaJeK naOei JIHaJ eaMeM anoOe OaSXR anXon
ioSen onQPe XHXXi JoQPi aOaMa noOae SXroQ iJieK iaDer
MiaVe JJaDH nXaVe JSHon aSoQP eeraS eODre JHSXR aeDao
naBBa QoOeH naQiJ ieKia OaXhr aaDDe naOae SXroQ iJieK
iaeLL eMiSX oIHeJ DeBBo ViJeK noSir aJJeK roXHX XoeVa

QeraH	naMoJ	XaHnr	eVira	nnoSH	LiXoi	OieiD	iQQoJ	iJeXX
orino	raKaB	BiaMe	XeSLa	KJiaX	oQera	HnaMo	JXaHn	DeBBo
ViJeK	nonon	eraHn	JeKno	ViJHS	SoOaH	nSeOD	JiQeD	eBBoV
aQaXa	SXaVi	IHeJJ	iQPeV	inMer	noSiO	eXXon	oneJJ	eSXHF
eenei	QaOin	eXXiD	eraQQ	enVer	eiJFH	oQoeD	erriS	QaJVa
reJeS	XanBe	nonSo	QoOea	nVaSS	eOaiJ	FaXXo	KJieQ	PeHnL
eJKio	rnoIH	eSXoD	eBBoV	iJeKn	oQaDi	XoneJ	JaLoX	XeKaV
iHnMe	QQPio	FaJeK	naOei	JIHaJ	eaMeM	anoOe	OaSXR	anXon
ioSen	onQPe	XHXXi	JoQPi	aOaMa	noOae	SXroQ	iJieK	iaDer
MiaVe	JJaDH	nXaVe	JSHon	aSoQP	eeraS	eODre	JHSXr	aeDao
naBBa	QoOeH	naQiJ	ieKia	OaXhr	aaDDe	naOae	SXroQ	iJieK
iaeLL	eMiSX	oIHeJ	DeBBo	ViJeK	noSir	aJJek	roXHX	XoeVa

X=t

QeraH	naMoJ	taHnr	eVira	nnoSH	Litoi	OieiD	iQQoJ	iJett
orino	raKaB	BiaMe	teSLa	KJiat	oQera	HnaMo	JtaHn	DeBBo
ViJeK	nonon	eraHn	JeKno	ViJHS	SoOaH	nSeOD	JiQeD	eBBoV
aQata	StaVi	IHeJJ	iQPeV	inMer	noSim	etton	oneJJ	eStHF
eenei	QaOin	ettiD	eraQQ	enVer	eiJFH	oQoeD	erriS	QaJVa
reJeS	tanBe	nonSo	QoOea	nVaSS	eOaiJ	Fatto	KJieQ	PeHnL
eJKio	rnoIH	eStoD	eBBoV	iJeKn	oQaDi	toneJ	JaLot	teKaV
iHnMe	QQPio	FaJeK	naOei	JIHaJ	eaMeM	anoOe	maStr	anton
ioSen	onQPe	tHtti	JoQPi	aOaMa	noOae	StroQ	iJieK	iaDer
MiaVe	JJaDH	ntaVe	JSHon	aSoQP	eeraS	eODre	JHStr	aeDao
naBBa	QoOeH	naQiJ	ieKia	OatHr	aaDDe	naOae	StroQ	iJieK
iaeLL	eMiSt	oIHeJ	DeBBo	ViJeK	noSir	aJJek	rotHt	toeVa

					aMeM	anoOe	OaStr	anton
ioSen	onQPe	tHtti	JoQPi	aOaMa	noOae	StroQ	iJieK	iaDer

M=v, S=s, O=m.....

la sostituzione è

a b c d e f g h i j k l m n o p q r s t u v w x y z
G L Q V A F K P U - - J O T Y D I N S X H M - - - B

il testo in chiaro è:

cerau navol taunr edira nnosu bitoi mieip iccol ilett
orino ragaz ziave tesba gliat ocera unavo ltaun pezzo
dileg nonon eraun legno dilus somau nsemp licep ezzod
acata stadi quell iched inver nosim etton onell estuf
eenei camin ettip eracc ender eilfu ocoep erris calda
reles tanze nonso comea ndass email fatto gliec heunb
elgio rnoqu estop ezzod ilegn ocapi tonel labot tegad
iunve cchio faleg namei lqual eavev anome mastr anton
iosen onche tutti lochi amava nomae stroc ilieg iaper
viade llapu ntade lsuon asoch eeras empre lustr aepao
nazza comeu nacil iegia matur aappe namae stroc ilieg
iaebb evist oquel pezzo dileg nosir alleg rotut toeda

cifrario di Vigenère

- è un cifrario polialfabetico
- m un intero positivo - sarà la lunghezza della chiave
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
- se $k = (k_1, k_2, \dots, k_m)$ si ha
 - $e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
 - $d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$
- tutto modulo 26
- esempio: sia $m = 5$ e $k = (5, 8, 14, 17, 4)$
- se $x = (4, 0, 17, 17, 8)$, allora $e_k(x) = (9, 8, 5, 8, 12)$
- la crittoanalisi è molto più difficile!