Le CryptoWars

Laboratorio di Matematica Industriale e Crittografia

Massimiliano Sala

Università di Trento, Dipartimento di Matematica

CryptoWarsCamps, settembre 2011

Outline

Outline

Le CryptoWars

Cosa sono?

Cosa coso?

- sono un'iniziativa del Laboratorio di Matematica Industriale e Crittografia (Universit[U+00E0] di Trento) a scopo divulgativo;
- singoli appassionati o team si scontrano creando codici e rompendo i codici degli altri!

Team di studenti universitari sono particolarmente benvenuti.

Outline

Sponsors

Le nostre Wars sono possibili solo grazie alla presenza di sponsors illuminati, che ringraziamo calorosamente.

- Alpha Orionis Srl, Milano, azienda attiva nella sicurezza in ambito Finance

alpha orionis

- Ceremit Srl, Thiene , azienda specializzata in Consulting Engineering

CONFIDACE

- SeeWeb, il piu' grande cloud provider interamente italiano

seeweb
HIGH QUALITY HOSTING

Patrocinanti

Clusit
Associazione Italiana per la Sicurezza Informatica

UNIVERSITÀ DEGLI STUDI DI TRENTO

UNIVERSITÀ DEGLI STUDI DI TORINO
ALMA UNIVERSITAS TAURINENSIS

unige
UNIVERSITÀ DEGLI STUDI DI GENOVA

UNIVERSITÀ DEGLI STUDI DI MILANO
www.dti.unimi.it
SEDE DI CREMA

UNIVERSITA' DEGLI STUDI
- UDINE -

Outline

La Gara

Date e tempistica

Allo scopo di diffondere e suscitare l'interesse nella Crittografia, organizziamo le CryptoWars2011, ovvero una competizione di crittografia a livello nazionale.

- 12 settembre 2011: inizio iscrizioni;
- 7 ottobre 2011: termine iscrizioni;
- 17 ottobre 2011: INIZIO gara;
- 12 marzo 2011: FINE gara;
- 19 marzo 2011: premiazione dei vincitori al Workshop BunnyTN.

Le Categorie

La gara [U+00E8] divisa in tre categorie. I concorrenti, che possono essere team o singoli, possono partecipare a una o pi [U+00F9] delle tre categorie.

Categorie

1. Categoria CLASSICA
2. Categoria CHIAVE PUBBLICA
3. Categoria CHIAVE PRIVATA

Outline

Il cifrario di Cesare

Uno dei metodi di crittatura pi[U+00F9] antichi [U+00E8] quello dovuto a Cesare.

Consideriamo l'alfabeto:

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

Dato un messaggio in chiaro, ciascuna lettera viene sostituita con quella che sta n passi dopo (nell'alfabeto).

Se prendiamo $n = 3$, CIAO viene crittato in FLDR.

Permutazione dell'alfabeto

Dato un alfabeto:

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	(space)	.	,	;	:	'	!	?

Una permutazione [U+00E8] un riarrangiamento dei simboli dell'alfabeto.

Le Permutazioni

Example (Permutazione)

Una semplice permutazione [U+00E8] shiftare i simboli dell'alfabeto di una posizione verso sinistra.

$$
\begin{array}{ccc}
\mathrm{a} & \rightarrow & \mathrm{b} \\
\mathrm{b} & \rightarrow & \mathrm{c} \\
\mathrm{c} & \rightarrow & \mathrm{d} \\
\mathrm{d} & \rightarrow & \mathrm{e} \\
\mathrm{e} & \rightarrow & \mathrm{f} \\
\mathrm{f} & \rightarrow & \mathrm{g} \\
\ldots & \rightarrow & \ldots \\
\ldots & \rightarrow & \ldots \\
! & \rightarrow & ? \\
? & \rightarrow & \mathrm{a}
\end{array}
$$

Il cifrario Monoalfabetico

Un cifrario Monoalfabetico usa una sola permutazione dell'alfabeto.

Example (Monoalfabetico)

Consideriamo la permutazione dell'esempio precedente.

CIAO(space)A(space)TUTTI diventa:

DJBP.B.UVUUJ

Il cifrario Polialfabetico Semplice

Invece che scegliere una sola permutazione dell'alfabeto, possiamo scegliere m permutazioni.

Il testo in chiaro viene diviso in blocchi di m simboli, chiamati word.

Il primo simbolo di ogni word viene crittato con la prima permutazione, il secondo con la seconda permutazione e cos [U+00EC] via.

Categoria CLASSICA

L'algoritmo

Ciascuna squadra che partecipa alla Categoria CLASSICA deve costruirsi un cifrario polialfabetico con 5 permutazioni ($m = 5$) per crittare un messaggio in chiaro.
L'alfabeto da considerare [U+00E8] quella presentato precedentemente con 34 simboli.

E' possibili usare 10 simboli speciali, che verranno indicati con i numeri 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Categoria CLASSICA

Polialfabetico con Varianti: i simboli speciali

Dato il testo in chiaro, gruppi di lettere o parole possono essere sostituite dai simboli speciali 1, 2, 3, 4, 5, 6, 7, 8, 9.

Quando il testo viene diviso in blocchi di 5 simboli ciascuno, questi non devono venir contati e non verranno neppure sostituiti dalle permutazioni (infatti i numeri non sono simboli dell'alfabeto).

Example

BUONA FORTUNA!, decidiamo che il numero 1 = NA.
Sostituisco le occorrenze di *TI* con il simbolo speciale:
BUO1(space)FORTU1! e dividiamo in blocchi di 5 simboli dell'alfabeto.

BUO1(space)F | ORTU1!

Categoria CLASSICA

Polialfabetico con Varianti: il simbolo speciale 0

Ogni squadra pu[U+00F2] usare il simbolo sepciale 0, per rappresentare un ulteriore regola a piacimento.

Ad esempio, mettere 0 davanti ad un word pu[U+00F2] semplicemente indicare che tale gruppo di lettere [U+00E8] stato invertito (0ITTUT sta ad indicare TUTTI).

Per evitare abusi, l'uso particolare dello zero deve essere approvato dagli organizzatori. Comunque nell'ultima fase della gara (l'attacco ai testi cifrati delle varie squadre) saranno resi noti i diversi possibili significati di tale simbolo (senza dire quale squadra usa quel significato)

Categoria CLASSICA

Esempio Pratico di Algoritmo

Scegliamo 5 permutazione dell'alfabeto: P_1, P_2, P_3, P_4 e P_5.
$P_1 = P_3 = P_5$ sono lo shift verso sinistra dell'alfabeto.
$P_2 = P_4$ la permutazione identit[U+00E0] (che lascia tutto invariato).

Vogliamo cifrare il testo in chiaro:

BUONA FORTUNA A TUTTE LE SQUADRE CHE PARTECIPANO ALLA GARA.

Categoria CLASSICA

Esempio Pratico di Algoritmo

Definiamo i simboli speciali:

- 1 = GL
- 2 = RA
- 3 = RE
- 4 = JI
- 5 = CD
- 6 = PC
- 7 = GN
- 8 = ZZ
- 9 = TT

Categoria CLASSICA

Esempio Pratico di Algoritmo

Sostituendo al messaggio in chiaro i simboli speciali:

BUONA|(space)FORT|UNA(space)A|(space)TU9E(space)|
LE(space)SQ|UAD3(space)C|HE(space)PA|RTECI|
PANO(space)|ALLA(space)|GA2.

crittato:

CUPNB|.FPRU|VNB(space)B|.TV9E.|ME.SR|VAE3(space)D|
IE.PB|RTFCJ|QAOO.|BLMA.|HA2,

Categoria CLASSICA

Esempio Pratico di Algoritmo

Possiamo ora decidere di inserire il simbolo speciale 0 per indicare l'inversione dei word crittati.

CUPNB|0URPF.|VNB(space)B|.TV9E.|ME.SR|VAE3(space)D|
IE.PB|RTFCJ|QAOO.|0.AMLB|HA2,

Categoria CLASSICA

Regolamento

Questa gara [U+00E8] composta da 3 fasi:

1 fase Preparazione dell'algoritmo di crittazione:
ogni squadra deve decidere quale algoritmo usare.

Entro il 7 ottobre 2011 deve essere spedito a mathnow.unitn@gmail.com:

- 5 permutazioni dell'alfabeto;
- i gruppi di lettere corrispondenti ai simboli speciali $(1 \ldots 9)$;
- il significato dello 0.

Categoria CLASSICA

Regolamento

2 fase Crittazione del testo in chiaro:
dopo il 7 ottobre, non appena la squadra avr[U+00E0] inviato il proprio cifrario a mathnow.unitn@gmail.com, questa ricever[U+00E0] un messaggio in chiaro tra crittare con il proprio algoritmo.

Il messaggio cifrato deve essere rispedito all'indirizzo di posta elettronica entro il 17 ottobre 2011.

Categoria CLASSICA

Regolamento

3 fase Attacco degli altri testi crittati.
dal 17 ottobre 2011 sul sito internet saranno disponibili i testi cifrati delle altre squadre da attaccare.

Quando una squadra riesce a decifrare un testo, questa deve spedite il testo in chiaro a mathnow.unitn@gmail.com indicando anche la squadra a cui appartiene il cifrato.
Gli organizzatori convalideranno l'attacco rimuovendo il testo cifrato da quelli disponibili da attaccare.
Questa fase si svolge dal 17 ottobre 2011 al 12 marzo 2012.

Categoria CLASSICA

Punteggio

- Ogni squadra parte con un punteggio iniziale di 20 punti.
- Se la squadra X riesce a decifrare il testo cifrato della squadra Y, X guadagna 10 punti, Y ne perde 20.
- Sul sito saranno messe a disposizione delle semplici “sfide“. Ogni squadra pu[U+00F2] provare ad attaccarne al massimo una e guadagnare 2 punti.
- Il vincitore [U+00E8] il team che ha totalizzato il punteggio maggiore.
- In caso di pareggio, verr[U+00E0] considerata vincitrice la squadra che per prima ha raggiunto tale punteggio.

Outline

Categoria CHIAVE PUBLICA

Regolamento e Punteggio

Prepareremo una serie di chiavi publiche da rompere, di difficolt[U+00E0] crescente e quindi con punteggio diverso.

Il 17 ottobre 2011, almeno 16 chiavi (in maggior chiavi RSA, ma anche di altri crittosistemi) verranno fornite ad ogni squadra.

Ogni squadra deve cercare di trovare la chiave privata dei crittosistemi a partire da quelle publica usando tutti i mezzi a loro disposizione. Quando una chiave viene rotta, la sua chiave privata deve essere spedita a mathnow.unitn@gmail.com. Vengono assegnati dei punti alla squadra e la chiave viene ritirata.
Questa gara si conclude il 12 marzo 2011.

L'algoritmo RSA

Alice  vuole trasmettere il messagio m a Bob  .

- Bob deve creare una chiave publica $K_{p,b} = (N, e)$ ed una privata $K_{s,b} = (N, d)$ stando attento a non divulgare d
- Bob trasmette (N, e) ad Alice

L'algoritmo RSA

- Bob sceglie due numeri primi p e q, molto grandi e li moltiplica $N = p \cdot q$
- Bob sceglie un numero e, coprimo con $\varphi(N)$ e pi[U+00F9] piccolo di $\varphi(N) = (p-1) \cdot (q-1)$
- Bob calcola d tale che
  $e \cdot d \equiv 1 \mod (p-1) \cdot (q-1)$
  d [U+00E8] l'inverso moltiplicativo di e
- solo Bob  conosce la chiave segreta (N, d) mentre (N, e) [U+00E8] publica

L'algoritmo RSA

Come avviene la cifratura e decifratura?

- Alice calcola $c = m^e \mod N$
- Alice trasmette c a Bob
- Bob riceve c e lo decripta calcolando:

$$c^d \equiv m \mod N$$

Infatti: $c^d \equiv m^{e \cdot d} \equiv m^{1+h \cdot \varphi(N)} \equiv m^1 \cdot \left(m^{\varphi(N)}\right)^h \equiv m \mod N$

$\xrightarrow{(N,e)}$

$\xrightarrow{c}$

Categoria CHIAVE PUBLICA

Le Chiavi

- chiavi publiche per RSA
  - alcune di lunghezza crescente da 100 bit in su;
  - alcune lunghe fino a 1000 bit, ma "deboli".
- chiavi pubbliche per ECC
- chiave pubblica per HCC
- chiave pubblica di HFE
- chiave pubblica su reticoli (NTRUE)

Outline

Categoria CHIAVE SIMMETRICA

Regolamento

L'obbiettivo di ciascuna squadra [U+00E8] quello di trovare un attacco il pi[U+00F9] efficace e veloce possibile al cifrario BunnyTN.

A partire dal 17 ottobre 2011 sul sito internet saranno reperibili le specifiche del cifrario.

Verranno premiati i migliori attacchi o tentativi di attacco sul crittosistema.
A parit[U+00E0] di strategia di attacco verr[U+00E0] premiato quello che [U+00E8] riuscito a rompere il maggior numero di round dell'algoritmo.

Categoria CHIAVE SIMMETRICA

Regolamento

Tutti i tipi di attacco e scenario sono i benvenuti.

Alcuni esempi di attacchi che si possono trovare in letteratura sono i seguenti:

- Key-recovery attacks: attacchi che cercano di ricostruire la chiave secreta dell'algoritmo (l'esempio pi[U+00F9] semplice [U+00E8] fare una ricerca esaustiva di tutte le chiavi possibili).
- Distinguishing attacks: attacchi che cercano di distinguere informazioni crittate da messaggi random.

Categoria CHIAVE SIMMETRICA

Regolamento

A seconda del tipo di informazioni che l'attaccante possiede, si possono definire diversi scenari:

- Related-key attacks
- Chosen-plaintext attacks
- Known-plaintext/ciphertext attacks
- Chosen-ciphertext attacks

GRAZIE DELL'ATTENZIONE

Clusit
Associazione Italiana per la Sicurezza Informatica

alpha orionis

CONFIDACE

seeweb
HIGH QUALITY HOSTING

UNIVERSITÀ DEGLI STUDI DI TRENTO

UNIVERSITÀ DEGLI STUDI DI TORINO
ALMA UNIVERSITAS TAURINENSIS

UNIVERSITÀ DEGLI STUDI DI MILANO
www.dti.unimi.it
SEDE DI CREMA

UNIVERSITA' DEGLI STUDI
- UDINE -

unige
UNIVERSITÀ DEGLI STUDI DI GENOVA