Appunti di Crittografia

Simone Ianniciello

A.A. 2020/2021

Contents

Chapter 1

Introduzione

1.1 La crittologia

La crittografia e' lo studio delle tecniche matematiche per:

Crittografia Metodi di cifratura.

Crittoanalisi Metodi di interpretazione.

Crittografia + Crittoanalisi = **Crittologia**

1.1.1 Scenario

A vuole spedire un messaggio a B, ma E sta' ascoltando il messaggio. Per proteggere la comunicazione, A e B utilizzano dei metodi di cifratura.

1.1.2 Cifratura

MSG	Insieme dei messaggi in chiaro
CRITTO	Insieme dei crittogrammi
C: MSG $\rightarrow$ CRITTO	Funzione di crittazione.
D: CRITTO $\rightarrow$ MSG	Funzione di decrittazione.

C e D sono una l'inversa dell'altra: $D(c) = D(C(m)) = m$
C e' iniettiva (messaggi diversi corrispondono a crittogrammi diversi).

1.2 Classificazione dei cifrari

I cifrari si dividono in:

Cifrari per uso ristretto Le funzioni C e D devono essere segrete; Poco pratici per la crittografia *di massa*.

Cifrari per uso generale Si basano su un metodo a chiave. C e D sono pubbliche ma la chiave deve essere nota ai soli interessati del messaggio.

1.2.1 Cifrari per uso generale

Le definizioni di C e D diventano:
C: MSG * KEYS → CRITTO
D: CRITTO * KEYS → MSG

Se un crittoanalista entra in possesso di una chiave, basta cambiarla. Esempi di cifrari a chiave segreta: 3DES, RC5, IDEA, AES.

Attacco esauriente (bruteforce) Il crittoanalista dovrebbe provare tutte le chiavi finché non trova quella giusta per decrittare il messaggio. Quasi impossibile da effettuare su chiavi abbastanza grandi (>20chars).

1.3 Attacchi

Gli attacchi possono avere successo completo (Si scopre la funzione D, compresa di chiave), oppure possono avere successo limitato (Si scopre solo qualche informazione su un messaggio).

1.3.1 Attacchi al sistema crittografico

Cypher Text Attack	Il crittoanalista rileva una serie di crittogrammi $c_1, \ldots, c_r$.
Known Plain-Text Attack	Il crittoanalista conosce una serie di coppie $(c_1, m_1), \ldots, (c_r, m_r)$.
Chosen Plain-Text Attack	Il crittoanalista sceglie una serie di $m_1, \ldots, m_r$ e si procura i relativi $c_1, \ldots, c_m$.

1.3.2 Attacchi Man-In-The-Middle MITM

Il crittoanalista si inserisce nel canale di comunicazione e blocca tutti i messaggi diretti. Puo' anche sostituire i messaggi originali con dei messaggi propri.

Condizione normale	Attacco MITM
$A \rightleftarrows B$	$A \rightleftarrows E \rightleftarrows B$

1.4 Cifrari perfetti

I cifrari perfetti sono totalmente sicuri, ma richiedono operazioni molto complesse perciò sono usati solo in condizioni estreme. In essi m e c sono totalmente scorrelati tra loro.

1.4.1 One-Time Pad

E un cifrario perfetto ma ha svantaggi enormi che lo rendono quasi inutilizzabile:

- Richiedono una chiave segreta nuova e perfettamente casuale per ogni messaggio.
- La chiave deve essere lunga quanto il messaggio.

1.4.2 Cifrari sicuri

I cifrari che vengono utilizzati ad ora non sono cifrari perfetti ma sono dichiarati sicuri. Cio' significa che non sono mai stati violati prima d'ora perché richiedono la risoluzione di problemi matematicamente difficili (Non essendo mai stato dimostrato $P \not\equiv NP$ non siamo *certi* che siano inviolabili).

1.5 Cifrari in uso

1.5.1 AES

E' un cifrario simmetrico (la stessa chiave viene utilizzata per crittare e decrittare), a blocchi (il messaggio e' diviso in blocchi lunghi come il messaggio). E' pubblicamente noto e utilizzato per comunicazioni *non classificate*. Si utilizzano chiavi brevi (128 o 256 bit).