Introduzione

Capitolo 1

Il Modello Computazionale

1.1 L'avversario

Il tipico avversario con cui si ha a che fare quando si studiano cifrari o protocolli crittografici nel modello computazionale, è un avversario con risorse di calcolo *limitate*. Limitate nel senso che si sceglie di porre un limite alla potenza dell'avversario. Questo significa che: non avremo a che fare con un avversario che ha una potenza computazionale infinita o un tempo illimitato a disposizione. Sebbene siano stati ideati cifrari sicuri anche rispetto ad avversari non limitati[1], questi soffrono di vari difetti: come per esempio il fatto che è necessario che la chiave sia lunga quanto il messaggio e che sia utilizzabile una sola volta. Per rappresentare in modo formale un avversario con risorse di calcolo limitate, lo si può pensare come un algoritmo appartenente ad una particolare classe di complessità computazionale[2]. Da sempre si considerano efficienti gli algoritmi che terminano in un numero di passi polinomiale nella lunghezza dell'input, mentre si considerano inefficienti quelli che hanno una complessità computazionale maggiore. Può sembrare quindi naturale immaginare gli avversari come degli algoritmi che terminano in un numero polinomiale di passi rispetto alla lunghezza dell'input. Non bisogna però dimenticare che un avversario può sempre *indovinare* il segreto che cerchiamo di nascondere, o che cifriamo. Per esempio: se il segreto che si cerca di nascondere ha una lunghezza di n bit, l'avversario può sempre lanciare una moneta n volte e associare, via via, la testa della moneta al valore 1 e la croce al valore 0. La probabilità che l'avversario ottenga una stringa uguale al segreto è ovviamente di $\frac{1}{2^n}$. Questa probabilità tende a 0 in modo esponenziale al crescere della lunghezza del segreto. Ma per valori finiti di n questa

[1] one-time pad ne è un esempio lampante.

[2] un avversario è alla fine dei conti una macchina di Turing che esegue un algoritmo.

probabilità non sarà mai 0. È quindi più realistico cercare di rappresentare l'avversario come un'algoritmo che oltre a terminare in tempo polinomiale, abbia anche la possibilità di effettuare scelte random. Ecco quindi che il nostro tipico avversario è un algoritmo Polinomiale Probabilistico. È inoltre giustificato cercare di rendere sicuri[3] gli schemi crittografici, rispetto principalmente, a questo tipo di avversario. Con questa scelta si cerca di rispettare il più possibile un famoso principio di Kerckhoffs[4] che afferma:

> *Un cifrario deve essere, se non matematicamente, almeno praticamente indecifrabile.*

Non è quindi necessario dimostrare che un particolare schema crittografico sia inviolabile, ma basta dimostrare che:

- in tempi ragionevoli lo si può violare solo con scarsissima probabilità
- lo si può violare con alta probabilità ma solo in tempi non ragionevoli

In crittografia i concetti di *scarsa probabilità* e di evento *raro* vengono formalizzati attraverso la nozione di funzione trascurabile.

Definizione 1.1 *Funzione Trascurabile (negligible). Sia $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ una funzione. Si dice che μ è trascurabile se e solo se per ogni polinomio p esiste $C \in \mathbb{N}$ tale che $\forall n > C$: $\mu(n) < \frac{1}{p(n)}$.*

Un'altra definizione utile è la seguente:

Definizione 1.2 *Funzione Notevole (noticeble). Sia $\mu : \mathbb{N} \rightarrow \mathbb{R}^+$ una funzione. Si dice che μ è notevole se e solo se esiste un polinomio p tale per cui esiste $C \in \mathbb{N}$ tale che $\forall n > C$: $\mu(n) > \frac{1}{p(n)}$.*

Per esempio la funzione $n \rightarrow 2^{-\sqrt{n}}$ è una funzione trascurabile, mentre la funzione $n \rightarrow \frac{1}{n^2}$ non lo è. Ovviamente esistono anche funzioni che non sono né trascurabili ne notevoli. Per esempio la seguente funzione definita per casi: $f(n) = \begin{cases} n/2, & \text{se } n \text{ è pari} \\ 3n+1, & \text{se } n \text{ è dispari} \end{cases}$
non è né trascurabile né notevole.

Se in un ipotetico esperimento ci si aspetta che un evento avvenga con una probabilt'a trascurabile, quest'evento dovrebbe verificarsi con una probabilità trascurabile anche se l'eseprimento è ripetututo molte volte, e quindi per la legge dei grandi numeri, con una frequenza altrettanto trascurabile [5]. In un

[3]In qualsiasi modo si possa intendere il concetto di sicurezza. Vedremo che in seguito si daranno delle definizioni rigorose di questo concetto.

[4]Auguste Kerckhoffs (19 Gennaio 1835 – 9 Agosto 1903) fu un linguista Olandese e un famoso crittografo

[5]In modo informale, la legge debole dei grandi numeri afferma che: per un numero grande di prove, la frequenza approssima la probabilità di un evento

modo pir̀igoroso si danno le seguneti definizioni:

Proposizione 1.1 *Siano* μ_1, μ_2 *due funzioni trascurabili e sia* $p(\cdot)$ *un qualsiasi polinomio. Se* $\mu_3 = \mu_1 + \mu_2$, *e* $\mu_4 = p(\cdot) \cdot \mu_1$, *allora* μ_3, μ_4 *sono funzioni trascurabili.*

Se quindi un evento avviene solo con una probabilità trascurabile in un esperimento, ci aspettiamo che ance se ripetiamo l'esperimento un numero polinomiale di volte la probabilità che l'evento avvenga rimanga comunque trascurabile. Supponiamo di avere un dado truccato in modo che la probabilità che, se lanciato, restituisca 1 è trascurabile. Allora se ripetiamo un numero polinomiale di volte quest'eseprimento, la probabilità che esca 1 in uno di questi esperimenti rimane comunque trascurabile. Gli eventi che avvengono con una probabilità trascurabile possono essere ignorati per fini pratici. In [KL07] infatti leggiamo:

> *Events that occur with negligible probability are so unlikely to occur that can be ignored for all practical purposes. Therefore, a break of a cryptographic scheme that occurs whit negligible probability is not significant.*

1.2 Indistinguibilità Computazionale

1.3 Dimostrazioni Basate su Games

1.4 Pseudocasualità

Capitolo 2

CryptoVerif

Capitolo 3

Risultati Raggiunti

Bibliografia

[KL07] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.