Sistemi di crittografia

Lezione 4 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2006-7

Indice

validità di sistemi di crittografia

caratteristiche di una crittografia valida secondo **Shannon (1949):**

1. la quantità di segretezza necessaria determina la quantità di lavoro necessaria per cifratura e decifrazione
2. l'insieme di chiavi e l'algoritmo di cifratura devono essere privi di complessità
3. l'implementazione del processo dovrebbe essere la più semplice possibile
4. gli errori di cifratura non dovrebbero propagarsi e danneggiare altre informazioni nel messaggio
5. la dimensione del testo cifrato non dovrebbe superare quella del testo in chiaro

criteri di validità di sistemi di crittografia **commerciale:**

- basata sulla matematica
- analizzata e giudicata efficace da esperti competenti
- ha superato la "prova del tempo"

sistemi di crittografia simmetrica e asimmetrica

terminologia:

- crittografia **simmetrica = a chiave segreta**
- crittografia **asimmetrica = a chiave pubblica**

differenza essenziale:

- crittografia simmetrica: $K_d = K_e$
  - unica chiave per cifratura e decifrazione
  - segreto **condiviso** da mittente e destinatario → **autenticazione**
- crittografia asimmetrica: $K_d \neq K_e$
  - chiavi distinte per cifratura e decifrazione
  - solo una delle due va tenuta segreta: segreto **locale**

problema inerente la crittografia simmetrica: **distribuzione delle chiavi**

problema inerente entrambi i tipi di crittografia: **gestione delle chiavi**

cifrature in successione e a blocchi

cifratura in successione: un simbolo alla volta

ad es.: cifratura per sostituzione

cifratura a blocchi: un blocco di simboli alla volta

ad es.: cifratura per trasposizione colonnare

confronto di algoritmi di cifratura in successione e a blocchi:

caratteristica	c. in successione	c. a blocchi
velocità di trasformazione	+	-
diffusione	-	+
limitazione della propagazione di errori	+	-
immunità a inserimenti maligni	-	+

criptoanalisi: tipi di attacco

in base alle informazioni di cui dispone, il criptoanalista può condurre un attacco a:

solo testo cifrato

il caso presupposto sinora (si usano: frequenze dei simboli nel testo cifrato e nel linguaggio, conoscenze acquisite, etc.)

testo in chiaro parziale o completo

si dispone di un messaggio cifrato e (di una parte) della sua decifrazione

attacco al testo in chiaro conosciuto

attacco al testo in chiaro probabile

testo cifrato di qualsiasi testo in chiaro

il criptoanalista può inserire testo in chiaro in input al processo di crittografia e osservare l'output: **attacco al testo in chiaro scelto**

algoritmo e testo cifrato

attacco al testo cifrato scelto

testo cifrato e testo in chiaro

obiettivo: dedurre la chiave

crittografia a chiave pubblica

idea originale: Diffie & Hellman (1976)

ma anche altri, contemporaneamente in Inghilterra: invenzione coperta dal segreto militare fino agli anni '90, v. Singh (1999)

ogni utente U ha una chiave **pubblica** K_{P_U} e un'associata chiave privata, o **segreta**, K_{S_U}

riservatezza: $M = D(K_{S_U}, E(K_{P_U}, M))$

autenticità: $M = D(K_{P_U}, E(K_{S_U}, M))$

è possibile assicurare **simultaneamente** riservatezza **e** autenticità in un sistema di crittografia a chiave pubblica?

sì! mediante **doppia cifratura:**

$$M = D(K_{S_B}, D(K_{P_A}, E(K_{S_A}, E(K_{P_B}, M))))$$