COME SCEGLIERE IL SISTEMA DI CIFRATURA PIÙ ADATTO?

Sistemi di cifratura a CHIAVE SEGRETA (simmetrica)

+ molto veloci
+ chiavi corte
- necessaria fiducia da e verso chi condivide la chiave
- è consigliabile cambiare la chiave ad ogni sessione, o comunque più spesso possibile
- Il numero di chiavi cresce velocemente col numero di utenti: una chiave per tutte le possibili coppie di utenti

Sistemi di cifratura a CHIAVE PUBBLICA (asimmetrica)

+ solo la chiave privata va mantenuta segreta
+ una coppia privata/pubblica può rimanere invariata per più sessioni
+ il numero di chiavi cresce meno in funzione del numero di utenti (una coppia per ogni utente)
- più lenti
- grandezza (in bit) delle chiavi almeno di un ordine di grandezza superiore

NUMERO DI UTENTI	NUMERO DI CHIAVI IN SISTEMI A CHIAVE PUBBLICA	NUMERO DI CHIAVI IN SISTEMI A CHIAVE PRIVATA
10	20	45
100	200	4590
1000	2000	455900
10000	20000	45559000

IN COMMERCIO

Tra gli algoritmi a chiave simmetrica più diffusi in commercio troviamo l'**AES (Advanced Encryption Standard)**, standard pubblico a partire dal 2001. Il suo principale impiego risiede nei protocolli di scambio sicuro (es. FTPS, HTTPS) per il flusso dei dati con le pagine web.

Tra gli algoritmi a chiave asimmetrica, il più diffuso è l'**RSA (Rivest, Shamir, Adleman)**, che prende il nome dai suoi ideatori. Questo viene spesso utilizzato per crittografare una chiave simmetrica da inviare a una seconda parte che l'ha richiesta. Riferendosi sempre al protocollo HTTPS, ad esempio, lo condivisione della chiave di sessione privata (AES) avviene proprio tramite l'algoritmo RSA.

CHIAVE PUBBLICA: FIRME DIGITALI

Oltre che per garantire la confidenzialità dei messaggi, le tecniche di cifratura a chiave pubblica possono essere utilizzate per realizzare la **firma digitale**. In tal caso il mittente utilizzerà la sua chiave privata per cifrare l'informazione, legando così la sua identità all'informazione trasmessa.

RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/crittografia/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

CIFRA LE TUE COMUNICAZIONI

Scopri cos'è la crittografia, perché è importante e come puoi usarla per proteggere le tue informazioni e le tue comunicazioni.

CRITTOGRAFIA

La **crittografia**, letteralmente "*scrittura segreta*", è l'arte, oggi la scienza, di nascondere i messaggi.

Nasce con lo scopo primario di garantire la confidenzialità dei dati, ma si è successivamente estesa anche ad altri scopi, come ad esempio quello di garantire l'integrità dei dati.
Essa permette di:

1. impedire modifiche non autorizzate mentre i dati sono memorizzati;
2. garantire che i dati trasmessi non siano comprensibili a chi li intercetti.

L'idea è quella di usare delle chiavi di cifratura per rendere incomprensibile (a chi non conosce tali chiavi) una certa informazione.

Dipendentemente dal fatto che le chiavi verde e viola (in figura) siano o meno la stessa chiave, si distinguono i due principali paradigmi in crittografia per cifrare una comunicazione:

- crittografia a **chiave segreta** (**crittografia simmetrica**);
- crittografia a **chiave pubblica** (**crittografia asimmetrica**).

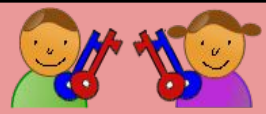
⚠ CANALE NON SICURO: qualsiasi mezzo di trasmissione in cui possibili intrusori potrebbero reperire l'informazione trasmessa.

CRITTOGRAFIA A CHIAVE SEGRETA

È, storicamente, la prima forma di crittografia, nata per comunicare:

- La **chiave di cifratura** è uguale alla **chiave di decifratura** (entrambe le parti la conoscono);
- implica che gli utenti abbiano la possibilità di scambiarsi la chiave in modo assolutamente **confidenziale**, evitando che questa possa essere intercettata.

L'antico "*Cifrario di Cesare*", che faceva corrispondere ogni lettera a quella di **tre** posizioni successive, è un esempio di crittografia a **chiave segreta**, in cui la chiave è proprio il "valore di mappatura" pari a **tre**.



CRITTOGRAFIA A CHIAVE PUBBLICA

Nata agli albori degli anni 70, è tutt'oggi un tema di ricerca molto attuale:

- La chiave di cifratura è diversa dalla chiave di decifratura;
- ogni utente ha una chiave **privata** (che conosce solo lui) e una chiave **pubblica** (che conoscono tutti);
- per cifrare il messaggio Bob usa la chiave pubblica di Alice e lo rinchiude in una "cassaforte", solo Alice potrà aprire la cassaforte con la sua chiave privata.

É usata principalmente per **scambiare chiavi** per sessioni private di comunicazione e per realizzare **firme digitali**.