1. INTRODUZIONE

Internet consente alle aziende di accedere facilmente alle informazioni, di ridurre i costi di comunicazione, di fornire un migliore servizio ai clienti, di effettuare commercio elettronico, etc. Tuttavia, esso espone i computer all'azione di attacchi da parte di malintenzionati: il numero di incidenti aumenta di anno in anno, e le perdite finanziarie hanno raggiunto livelli misurabili in miliardi di dollari.

Il ***CERT*** (***Computer Emergency Response Team***) è un team di esperti nell'ambito della sicurezza, creato dal ***DARPA*** (***Defense Advanced Research Projects Agency***) in seguito all'attacco del worm di Morris, il quale si occupa di: identificare il tipo di incidenti, quantificare le perdite economiche ed analizzare le vulnerabilità dei prodotti.

Gli attacchi informatici possono essere contrastati attraverso difese statiche e dinamiche. La difesa ***statica*** prima o poi cede dopo nuovi attacchi, per cui è opportuno adattarsi ***dinamicamente*** ai nuovi attacchi per avere maggiori possibilità. Questa è una proprietà anche degli attaccanti, in quanto (ad esempio) i virus ***polimorfici*** si modificano continuamente per evitare di essere rilevati; gli autori dei virus modificano, inoltre, algoritmi di mutazione dopo aver appreso le nuove tecniche di rilevazione. Bisogna essere costantemente aggiornati e rispondere subito alle novità.

Per "***vulnerabilità***" s'intende la debolezza di un sistema di sicurezza che può essere utilizzata per causare danni.
Un ***attacco*** è uno sfruttamento di una vulnerabilità di un sistema. Essi possono essere:

- ***passivi***, se non alterano i dati in transito (intercettazione/analisi del traffico, …)
- ***attivi***, se modificano il flusso di dati o creano un falso flusso (riproduzione, modifica dei messaggi, Denial of Service, …).

Gli ***obiettivi*** della sicurezza dati sono:

- La ***confidenzialità*** (o privacy/segretezza) vuole che le informazioni trasmesse e memorizzate siano accessibili in lettura solo da chi è autorizzato.
- L'***autenticazione*** può riferirsi a messaggi, entità e tempo.
- Il ***non-ripudio*** vuole che chi invia/riceve non possa negare la trasmissione del messaggio.
- Il ***controllo*** *degli accessi* vuole che l'accesso alle informazioni sia controllato da o per il sistema.
- L'***integrità*** vuole che solo chi è autorizzato possa modificare l'attività di un sistema o le informazioni trasmesse.
- L'***anonimia*** vuole garantire la protezione dell'identità o del servizio utilizzato.
- La ***disponibilità delle risorse*** vuole che le risorse siano disponibili solo a chi è autorizzato quando necessario.
- La ***Protezione Proprietà Intellettuale*** (DRM – Digital Rights Management) vuole controllare l'uso, la modifica e la distribuzione di dati soggetti a forme di copyright.

1.1 CRITTOGRAFIA

La **crittografia** è un meccanismo utilizzato dall'antichità fino a pochi anni fa: essenzialmente per comunicazioni private e usi militari/diplomatici. Oggi, essa coinvolge lo studio di tecniche ed applicazioni che dipendono dall'esistenza di problemi difficili.
Tra gli strumenti crittografici annoveriamo ***OpenSSL***, un progetto open source nato nel dicembre del 1998 che fornisce implementazioni per:

- funzioni crittografiche;
- protocolli SSL (Secure Sockets Layer) e TLS (Transport Layer Security).

OpenSSL comprende dei comandi eseguibili per funzioni crittografiche, oltre ad una libreria contenente API, mediante la quale i programmatori possono sviluppare le proprie applicazioni crittografiche. ***OpenSSL*** supporta crittografia basata su curve ellittiche (Elliptic Curve Cryptography).

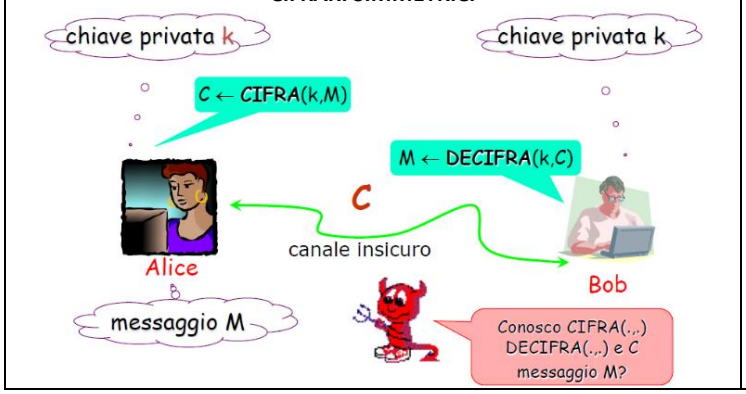
Cifrario:

In crittografia un ***cifrario*** (o cifra) è un algoritmo utilizzato per eseguire operazioni di ***cifratura*** e ***decifratura***, vale a dire una serie di passaggi ben definiti che possono essere seguiti come una procedura, volte a rendere oscuro, ossia semanticamente non leggibile, un testo di un messaggio in chiaro (plain text) o, al contrario, al ripristino in chiaro di un messaggio precedentemente cifrato. I cifrari possono essere:

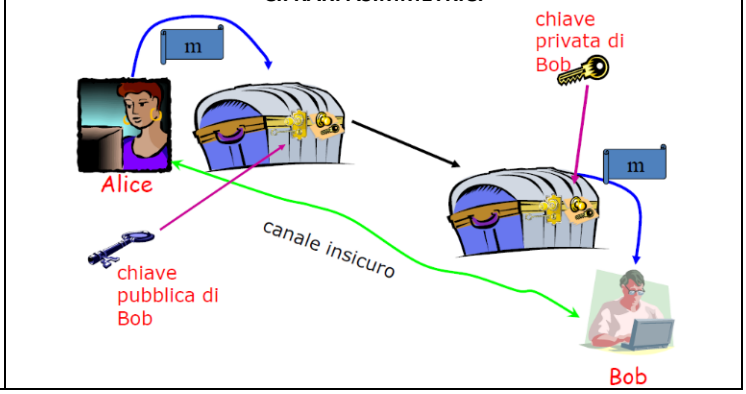
- **Simmetrici,** utilizzano una chiave privata condivisa tra mittente e destinatario del messaggio: esso viene cifrato prima dell'invio e decifrato alla ricezione. Tra i cifrari simmetrici annoveriamo i *cifrari a blocco* (DES, Triplo DES, AES, Blowfish, RC5, RC6, …) e gli *Stream Cipherr* (LSFR, RC4).
- **Asimmetrici**, usano una "cassaforte" con due lucchetti: con una chiave (***pubblica***) si chiude la cassaforte, con l'altra chiave (***privata***) si apre la cassaforte. Ovviamente, la chiave pubblica dev'essere diversa dalla privata.

Ad esempio, se Bob vuole inviare un messaggio ad Alice, egli consulta la chiave pubblica di quest'ultima, cifrando il messaggio ed inviandolo; alla ricezione, Alice utilizza la sua chiave privata e decifra il messaggio. Chiunque può cifrare un messaggio per Alice, ma solo alice può decifrare un messaggio cifrato per lei. Non ci sono chiavi condivise tra Alice e Bob: ciascuno dei due utenti genera da solo la propria coppia di chiavi e rende pubblica la chiave pubblica.
I cifrari simmetrici più utilizzati sono RSA, El Gamal e sistemi basati su curve ellittiche.

CIFRARI SIMMETRICI

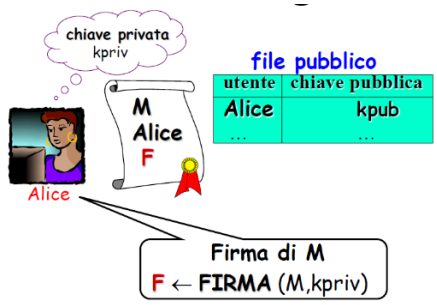


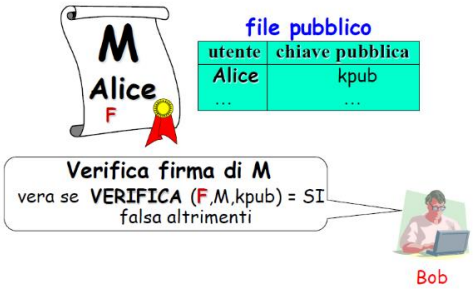
CIFRARI ASIMMETRICI



Firma digitare:

La **firma digitale** è equivalente alla firma convenzionale, ma deve poter essere facilmente prodotta dal legittimo firmatario: nessun utente deve poter riprodurre la firma di altri, ma chiunque può facilmente verificare una firma. Nella pratica, quando Alice vuole firmare un messaggio utilizza una chiave privata; alla ricezione, Bob in sostanza verifica se c'è una corrispondenza tra firma digitale e chiave pubblica di Alice.





Per la firma digitale, si utilizzano RSA, El Gamal, DSA e ECDSA (basato su curve ellittiche).

Per distribuire le chiavi pubbliche ed assicurare che una chiave pubblica è quella di un prefissato utente, entra in gioco la PKI: la **Public Key Infrastructure** è un insieme di hardware, software, procedure e politiche per creare, gestire, memorizzare, distribuire e revocare certificati digitali.

Funzioni Hash:

Una **funzione hash** è una funzione che riceve in input una lunghezza arbitraria/finita di bit e ne restituisce una di b bit. L'idea alla base è che il valore hash(M) è una rappresentazione non ambigua e non falsificabile del messaggio M. Trattasi di funzioni facili da computare, ed è altresì difficile trovare una collisione.

Le funzioni hash più comuni sono:

- MD5 (Message Digest Algorithm), valore di 128 bit;
- SHA-0, SHA-1 con 160 bit;
- SHA-2, cioè SHA-224, SHA-256, SHA-384, SHA-512 (Secure Hash Algorithm).

Ad esempio:

- SHA1("Cantami o diva del pelide Achille l'ira funesta") = 1f8a690b7366a2323e2d5b045120da7e93896f47;
- SHA1("C**o**ntami o diva del pelide Achille l'ira funesta") = e5f08d98bf18385e2f26b904cad23c734d530ffb.

Dagli esempi precedenti si nota subito che, nonostante si cambi una sola lettera di una stringa, la differenza tra i risultati ottenuti è abissale. Le funzioni hash si utilizzano per firme digitali, integrità dei dati e certificazione del tempo.

Per utilizzare un servizio, un utente deve autenticarsi. L'***autenticazione*** può avvenire attraverso qualcosa che l'utente POSSIEDE (oggetti fisici/elettronici, …), CONOSCE (password, PIN, …) oppure È (biometria, …); spesso si utilizza una combinazione dei precedenti tre meccanismi.

La **sicurezza sul Web** ricopre un ruolo importantissimo: ad oggi, oltre l'80% del traffico Web è cifrato mediante il protocollo HTTPS, come è emerso dall'analisi telemetrica dei due browser più diffusi (Chrome e Firefox). Questo risultato è stato ottenuto anche grazie alla scelta di utilizzare protocolli sicuri da parte dei principali social network e motori di ricerca.