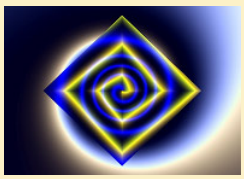
PFT 3 MAGGIO 2005

SICUREZZA E PRIVACY NELLA TRASMISSIONE DATI ATTRAVERSO LA RETE PUBBLICA INTERNET: QUALI RESPONSABILITÀ



Ing. Ermanno Ancona CED Centro di Medicina Preventiva Az. ULSS 20 VERONA

DROnet
Network Nazionale sulle Dipendenze

Piano di Formazione Tossicodipendenze

LA SICUREZZA PRINCIPALMENTE E'.....

- DOTARSI DI UN FIREWALL
- DOTARSI E MANTENERE AGGIORNATO UN ANTIVIRUS
- DOTARSI DI ANTI SPY-WARE
- UTILIZZARE UN PARTICOLARE SISTEMA OPERATIVO
- MANTENERE AGGIORNATO IL SW UTILIZZATO
- MANTENERSI INFORMATO
- AFFIDARSI A BRAVI TECNICI

LA SICUREZZA PRINCIPALMENTE E'....

UN ATTEGGIAMENTO MENTALE

DUE COMPORTAMENTI CONTRAPPOSTI

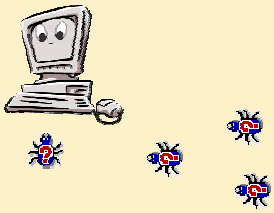
IN MEDIO STAT VIRTUS

(Orazio)

LA RETE ASSOMIGLIA ……..

…. AL MONDO CHE CI CIRCONDA

ADOTTIAMO INNANZITUTTO GLI STESSI CRITERI DI VALUTAZIONE E IL BUON SENSO DELLA VITA DI TUTTI I GIORNI….



I PROTOCOLLI DI COMUNICAZIONE

I DATI SULLE RETE VIAGGIANO IN CHIARO

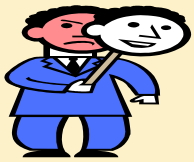
….AD ESEMPIO INVIARE UN'EMAIL EQUIVALE PRATICAMENTE AD INVIARE UNA CARTOLINA

ALCUNI PERICOLI

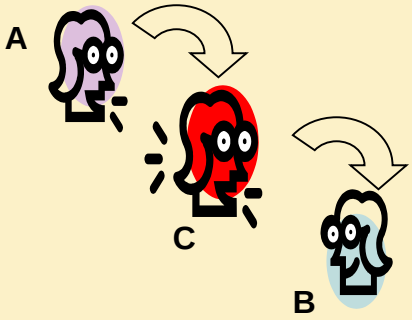
SNIFFING

dati in transito sulla rete

SPOOFING



MAN IN THE MIDDLE



PHISHING

LE NOSTRE ESIGENZE SONO……

CHE L'INFORMAZIONE ABBIA CARATTERISTICHE DI:

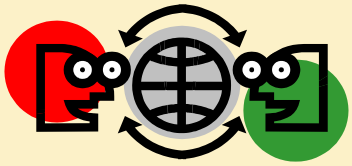
- **CONFIDENZIALITÀ**
- **INTEGRITÀ**
- **AUTENTICITÀ**

(non ripudiabilità)

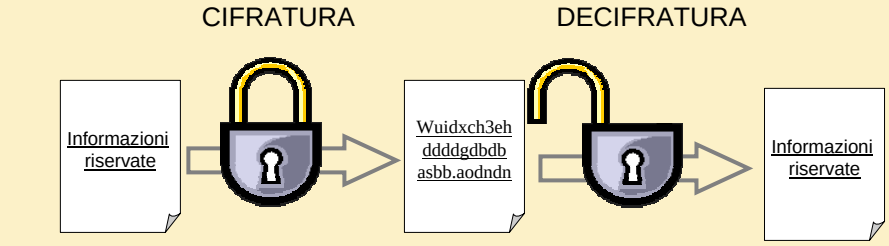
UNA RISPOSTA ALLE NOSTRE ESIGENZE

CRITTOGRAFIA: lo studio di tecniche matematiche che possano garantire la sicurezza delle informazioni

Il problema della confidenzialità delle informazioni nasce in particolare nelle attività belliche e con la crittografia i messaggi vengono modificati in modo che non siano più intellegibili al nemico



SCHEMA DI CRITTOGRAFIA



ELEMENTI BASE DEL PROCESSO

La trasformazione del testo avviene attraverso una chiave segreta la sicurezza dipende:

- dalla bontà dell'**ALGORITMO**

- dalla segretezza della **CHIAVE**

IL CIFRARIO DI CESARE

Esempio banale di cifratura convenzionale: sostituiamo una parte di informazione con un'altra

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

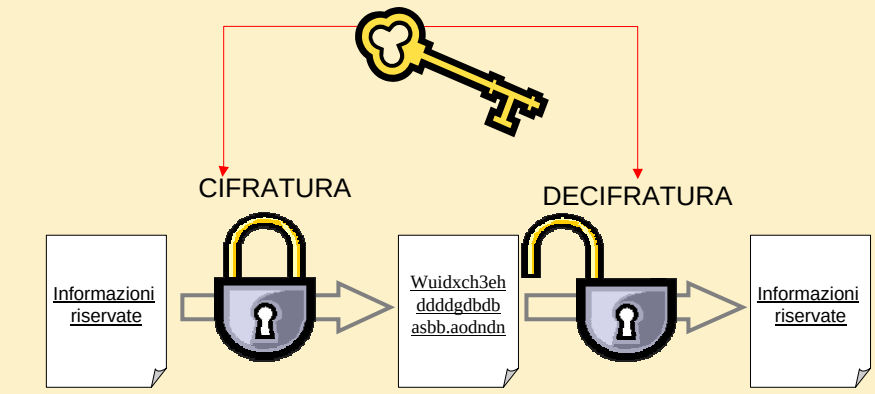
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Operiamo uno slittamento di 3 caratteri A=D B=E C=F .....

CIAO = **FLDR**

L'ALGORITMO È: SLITTA I CARATTERI
LA CHIAVE È: 3

LA CRITTOGRAFIA SIMMETRICA

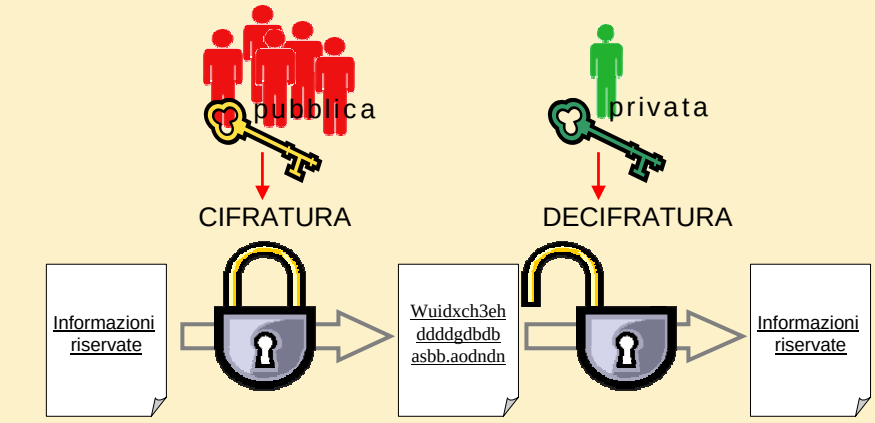


TESTO IN CHIARO **TESTO CIFRATO** **TESTO IN CHIARO**

LA CRITTOGRAFIA SIMMETRICA

- Utilizza la **medesima chiave** per cifrare e decifrare i dati.
- Ciò presuppone che sia il mittente che il destinatario delle informazioni conoscano la chiave segreta.
- La principale debolezza di questo sistema risiede proprio nello **scambio della chiave** segreta qualora le due parti siano fisicamente distanti e debbano utilizzare un canale di comunicazione insicuro.
- Chiunque riesca ad intercettare la chiave in transito potrà poi **decifrare**, **modificare** e **falsificare** i dati trasmessi.

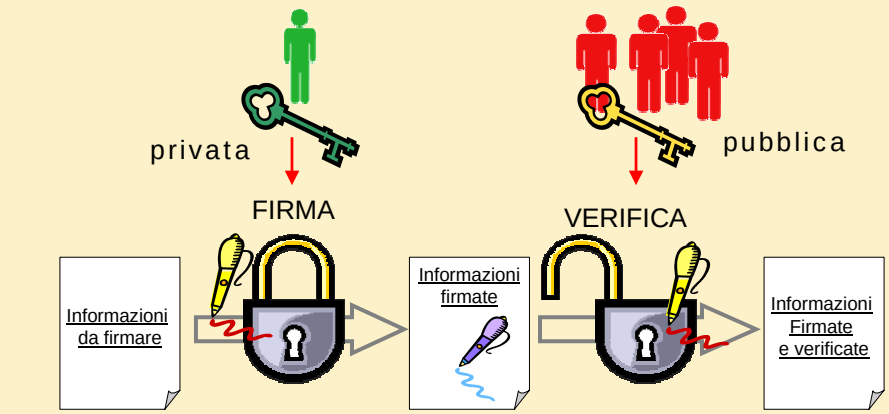
LA CRITTOGRAFIA ASIMMETRICA



LA CRITTOGRAFIA ASIMMETRICA

- Utilizza una coppia di chiavi: la **chiave pubblica** cifra i dati e solamente la corrispondente **chiave privata** è in grado di decifrarli.
- La **chiave pubblica** può essere tranquillamente **distribuita** mentre la **chiave privata** deve essere **custodita** dal proprietario.
- Non esiste (al momento non è noto) un processo computazionale che permetta di determinare la chiave privata a partire da quella pubblica
- Chiunque voglia comunicarmi della informazioni potrà usare la mia chiave pubblica per cifrarle: **SOLO IO** utilizzando la mia chiave privata sarò in grado di decifrarle.

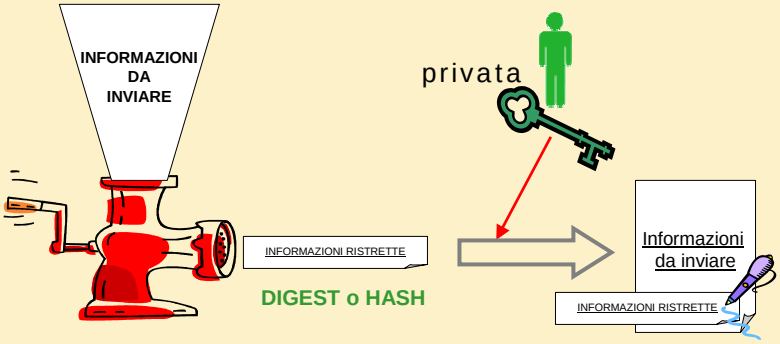
DIGITAL SIGN (FIRMA DIGITALE)



TESTO IN CHIARO **TESTO FIRMATO** **TESTO VERIFICATO**

ALGORITMI DI HASH (l'integrità)

TESTO IN CHIARO



FUNZIONE DI HASH

TESTO IN CHIARO PIU' FIRMA

INTEGRITA' E AUTENTICITA'

L'unione fa' la forza…….

INVIO:

1. dato il documento ricavo il suo **hash**
2. con la **mia chiave privata** cifro l'hash del documento

RICEZIONE:

1. chi riceve con la **mia chiave pubblica** decifra l'hash
2. calcola in maniera indipendente l'hash del documento
3. confronta i 2 hash

LE CA (Certification Athority)

Se i soggetti con cui comunico sono molti e non li conosco di persona si pongono alcuni problemi:

Q. Dove trovo le chiavi pubbliche?

A. Creazione di archivi di chiavi pubbliche, public key server.

Q. Chi mi assicura che la chiave pubblica appartenga al proprietario dichiarato?

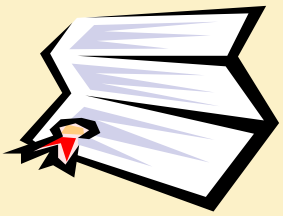
A. Ci pensano le C.A. sono enti certificatori.

……e poi……IN C.A. WE TRUST

I CERTIFICATI

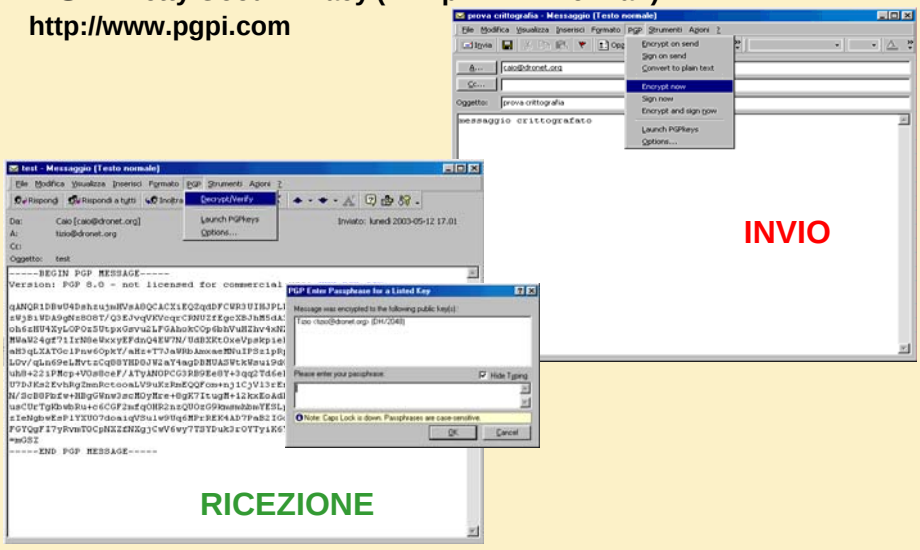
Sostanzialmente sono costituiti da:

1. **La chiave pubblica della persona o ente**
2. **I dati della persona o ente**
3. **Il tutto firmato con la chiave privata dell'ente certificatore**



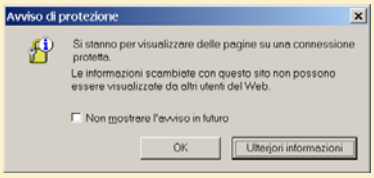
APPLICAZIONE PRATICA: E-MAIL

PGP Pretty Good Privacy (Philip R. Zimmerman)
http://www.pgpi.com

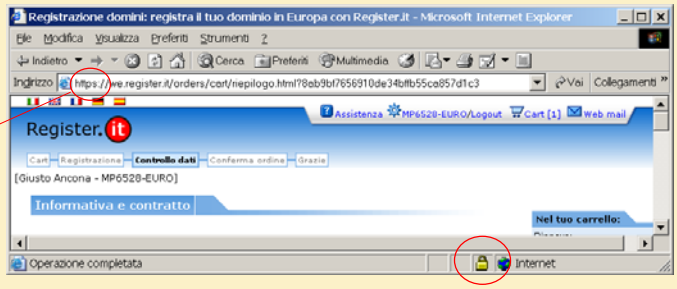


APPLICAZIONE PRATICA: NAVIGAZIONE

SSL Secure Socket Level



HTTPS



APPLICAZIONE PRATICA: SSL

Come lavora il browser standard: ha già le chiavi pubbliche delle CA più note per verificare il certificato (mi devo fidare del produttore del browser)

IPOTESI 1

1. il mio browser si collega ad un server che gli invia il proprio certificato
2. il mio browser verifica se il certificato corrisponde ad una CA che conosce
3. se si, verifica la validità del certificato del sito web
4. se la verifica è positiva crea il tunnel cifrato e mostra le pagine, compare il lucchetto nella barra di stato del browser, compare https:// nell'indirizzo
5. se la verifica fallisce il browser mi avvisa e chiede cosa fare

IPOTESI 2

1. il mio browser verifica che il certificato non corrisponde ad una CA che conosce
2. mi mostra i dati del certificato e mi chiede se voglio proseguire
3. posso memorizzare il certificato per la prossima volta

RESPONSABILITÀ

- Trattamento illecito di dati personali e/o sensibili
- Omessa adozione delle misure minime di sicurezza per i sistemi informativi

Fonti normative e documenti:

Decreto legislativo 30 giugno 2003, n. 196
Codice in materia di protezione dei dati personali

Allegato B disciplinare tecnico in materia di misure minime di sicurezza

(Artt. da 33 a 36 del codice)

BIBLIO-WEBOGRAFIA (essenziale)

- An Introduction to Cryptography, Network Associates Inc. 2000
- Aspetti di crittografia moderna da DES alla crittografia quantistica, Andrea Pasquinucci
- www.philzimmermann.com
- www.ietf.org/rfc/rfc2440.txt
- www.ietf.org/rfc/rfc2246.txt
- www.ietf.org/rfc/rfc2818.txt
- www.openpgp.org
- www.gnupg.org
- www.gnupg.org/it/gnupg.html
- www.pgpi.com
- www.rsasecurity.com/
- www.verisign.com
- www.openssl.org/
- www.apache-ssl.org/

CLUSIT- Associazione Italiana per la Sicurezza Informatica

www.clusit.it **info@clusit.it**

Associazione "no profit" con sede presso l'**Università degli Studi di Milano**

Dipartimento di Informatica e Comunicazione

In ambito nazionale, il CLUSIT opera in collaborazione con:

- Ministero delle **Comunicazioni**
- Ministero degli **Interni**
- Ministero dell'**Istruzione** dell'**Università** e della **Ricerca**
- Dipartimento per l'**Innovazione** e le **Tecnologie**
- **Polizia** Postale e delle Comunicazioni
- Autorità **Garante** per la tutela dei dati personali
- **A**utorità per le **G**aranzie nelle **C**omunicazioni
- **Federcomin** (Confindustria)
- **Università** e Centri di **Ricerca**
- **Associazioni** Professionali e Associazioni dei **Consumatori**.

CLUSIT- Associazione Italiana per la Sicurezza Informatica

OBIETTIVI:

Diffondere la **cultura della sicurezza informatica** presso le Aziende, la Pubblica Amministrazione e i cittadini.

Partecipare alla elaborazione di **leggi, norme** e **regolamenti** che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.

Contribuire alla definizione di percorsi di **formazione** per la preparazione e la **certificazione** delle diverse figure professionali operanti nel settore della sicurezza.

Promuovere l'uso di **metodologie** e **tecnologie** che consentano di migliorare il livello di sicurezza delle varie realtà.

Ing. Ermanno Ancona CED Centro di Medicina Preventiva Az. ULSS 20

CLUSIT- Associazione Italiana per la Sicurezza Informatica

FA PARTE DI UN NETWORK EUROPEO

CLUSIT	Italia
CLUSIS	Svizzera
CLUSIF	Francia
CLUSIB	Belgio
CLUSSIL	Lussemburgo

In collaborazione con le altre associazioni europee
Il CLUSIT partecipa a progetti dell'Unione Europea, consentendo ad aziende italiane di accedere ai finanziamenti europei.

Ing. Ermanno Ancona CED Centro di Medicina Preventiva Az. ULSS 20