

DOCUMENTO ELETTRONICO E FIRMA DIGITALE

CHE COSA È LA CRITTOGRAFIA

***LA CRITTOLOGIA È SCIENZA CHE STUDIA LE
“SCRITTURE SEGRETE”***

CRITTOGRAFIA

STUDIA I SISTEMI DI PROTEZIONE DEI MESSAGGI

CRITTOANALISI

STUDIA I METODI PER DECIFRARE UN MESSAGGIO CIFRATO

TESTO IN CHIARO

MESSAGGIO DI CUI SI VUOLE PROTEGGERE IL CONTENUTO

TESTO IN CIFRA O CIFRATO

MESSAGGIO TRASFORMATO E RESO INCOMPRESIBILE

LO SCOPO DELLA CRITTOGRAFIA È STATO PER SECOLI QUELLO DI NASCONDERE, PER MOTIVI DI SICUREZZA, INFORMAZIONI CONTENUTE IN MESSAGGI CON APPLICAZIONI PREVALENTI IN CAMPO MILITARE E DIPLOMATICO.

OGGI LA CRITTOGRAFIA VIENE USATA, OLTRE CHE PER LO SCOPO CLASSICO, ANCHE PER RISOLVERE FONDAMENTALI PROBLEMI CONNESSI CON L'UTILIZZO DEI MODERNI MEZZI DI COMUNICAZIONE DIGITALE IN PARTICOLARE QUELLI RIFERITI

- **ALL'IDENTIFICAZIONE DEI CORRISPONDENTI**
- **AUTENTICAZIONE DELLE INFORMAZIONI SCAMBIATE**

SI PASSA QUINDI

- ***DALLA CRITTOGRAFIA CHE NASCONDE***
- ***ALLA CRITTOGRAFIA CHE GARANTISCE***

IN ALTRE PAROLE

LA CRITTOGRAFIA SERVE A FORNIRE AUTENTICITÀ A

- ***IDENTITÀ DI UNA PERSONA***
- ***CONTENUTO E PROVENIENZA DI UN MESSAGGIO***

IL BUON FUNZIONAMENTO DI UN SISTEMA CRITTOGRAFICO HA FRA LE SUE COMPONENTI FONDAMENTALI, LA GESTIONE LOGISTICA DELLE CHIAVI DI CIFRATURA ED IN PARTICOLARE:

- ***LA GENERAZIONE***
- ***LA CONSERVAZIONE***
- ***L'ASSEGNAZIONE AI "PROPRIETARI"***
- ***LA CERTIFICAZIONE***

LA CRITTOGRAFIA NELLA COMUNICAZIONE ELETTRONICA

NELLA COMUNICAZIONE ELETTRONICA SI INDIVIDUANO DUE PROBLEMATICHE RILEVANTI CHE POSSONO ESSERE AFFRONTATE CON SUCCESSO CON TECNICHE CRITTOGRAFICHE:

- **LA RISERVATEZZA**
- **SICUREZZA**

RISERVATEZZA

AVERE LA CERTEZZA CHE IL CONTENUTO DEL MESSAGGIO POSSA ESSERE CONOSCIUTO SOLO DAL DESTINATARIO LEGITTIMO E NON DA ALTRI

SICUREZZA

AVERE LA CERTEZZA CHE TUTTO IL PROCESSO DI TRASMISSIONE DEL MESSAGGIO SIA:

- ***LEGITTIMO***
- ***CONFORME ALLE REGOLE***
- ***ESEGUITO DA CHI È LEGITTIMATO A FARLO***

LA SICUREZZA SI ARTICOLA SCHEMATICAMENTE IN:

IDENTIFICAZIONE	CERTEZZA DELL'IDENTITÀ DEL MITTENTE E DEL DESTINATARIO
AUTORIZZAZIONE	CERTEZZA DELLA LEGITTIMITÀ DELLA OPERAZIONE
AUTENTICAZIONE	CERTEZZA DELL'AUTENTICITÀ E DELL'INTEGRITÀ DEL MESSAGGIO

SISTEMA DI CRITTOGRAFIA A CHIAVE PUBBLICA

***SI BASA SU UN SISTEMA DI CIFRATURA ASIMMETRICO
VENGONO USATE DUE CHIAVI DISTINTE***

- ***UNA CHIAVE PER CIFRARE***
- ***UNA PER DECIFRARE***

CARATTERISTICHE PRINCIPALI DEL SISTEMA DI CIFRATURA ASIMMETRICO

- ***OGNI UTENTE POSSIEDE DUE CHIAVI DISTINTE***
- ***LA CHIAVE PER CIFRARE È DIVERSA DA QUELLA PER DECIFRARE***
- ***DALLA CONOSCENZA DI UNA CHIAVE NON SI PUÒ RISALIRE ALLA CONOSCENZA DELL'ALTRA***

CARATTERISTICHE PRINCIPALI DEL SISTEMA DI CIFRATURA ASIMMETRICO

- ***LA CHIAVE DI CIFRATURA O DIRETTA (CHIAVE PUBBLICA) CHE VIENE RESA NOTA ATTRAVERSO UN ELENCO***
- ***LA CHIAVE PER LA DECIFRAZIONE O INVERSA (CHIAVE PRIVATA) VIENE MANTENUTA SEGRETA DAL PROPRIETARIO***

FUNZIONAMENTO DEL SISTEMA DI CRITTOGRAFIA A CHIAVE PUBBLICA

PER SEMPLICITÀ CI SI RIFERISCE AL CASO DI DUE UTENTI

A E B

UTENTE A POSSIEDE

- **LA CHIAVE DIRETTA (DI CIFRATURA) A_d**
- **LA CHIAVE INVERSA (DI DECIFRATURA) A_i**

UTENTE B POSSIEDE

- **LA CHIAVE DIRETTA (DI CIFRATURA) B_d**
- **LA CHIAVE INVERSA (DI DECIFRATURA) B_i**

PRIMO CASO

A DEVE INVIARE UN MESSAGGIO A B IN MODO RISERVATO

- ***A CIFRA IL MESSAGGIO CON LA CHIAVE PUBBLICA DI B (B_d)***
- ***A INVIA IL MESSAGGIO A B***
- ***B DECIFRA CON LA PROPRIA CHIAVE INVERSA (B_i) IL MESSAGGIO***

DATA LA NATURA DELLE CHIAVI ASIMMETRICHE APPARE EVIDENTE CHE NESSUNO TRANNE B, POSSESSORE DELLA CHIAVE INVERSA, PUÒ LEGGERE IL MESSAGGIO

SECONDO CASO

A VUOLE INVIARE UN MESSAGGIO PUBBLICO IN CHIARO IN MODO CHE NE RISULTI L'AUTENTICITÀ

- **A** CIFRA IL MESSAGGIO CON LA PROPRIA CHIAVE PRIVATA (**A_i**)
- **A** INVIA IL MESSAGGIO

CHIUNQUE SIA INTERESSATO PUÒ LEGGERE IL MESSAGGIO DECIFRANDOLO CON LA CHIAVE PUBBLICA DI **A** (**A_d**) DISPONIBILE SU UN APPOSITO ELENCO.

APPARE EVIDENTE CHE IN QUESTO MODO È PROVATA L'AUTENTICITÀ DEL MESSAGGIO (CIOÈ IL FATTO CHE È STATO PRODOTTO DA **A**).

TERZO CASO

A VUOLE INVIARE IN MODO RISERVATO UN MESSAGGIO A B FIRMANDOLO

- **A CIFRA IL TESTO CON LA PROPRIA CHIAVE PRIVATA (A_i)**
- **A CIFRA, ULTERIORMENTE IL TESTO CON LA CHIAVE PUBBLICA DI B (B_d)**
- **A INVIA IL MESSAGGIO**
- **B APPLICA AL MESSAGGIO LE CHIAVE PUBBLICA DI A, ASSICURANDOSI COSÌ DELL'AUTENTICITÀ DELLA PROVENIENZA**
- **B APPLICA AL MESSAGGIO LA PROPRIA CHIAVE PRIVATA DECIFRANDOLO**

APPLICANDO TALE PROCEDURA SI HA LA CERTEZZA DELLA PROVENIENZA DEL MESSAGGIO E DELLA SUA RISERVATEZZA (PUÒ ESSERE LETTO SOLO DAL DESTINATARIO).

IL MECCANISMO DI FUNZIONAMENTO DELLA CRITTOGRAFIA A CHIAVE PUBBLICA SI BASA SU UN ELENCO CENTRALIZZATO E CONSULTABILE DA TUTTI CHE CONTENGA LE CHIAVI PUBBLICHE DEGLI UTENTI

SI APRONO ALCUNE QUESTIONI FONDAMENTALI

- ***CHI GESTISCE L'ELENCO DELLE CHIAVI PUBBLICHE?***
- ***CHI GARANTISCE DELL'AUTENTICITÀ (CORRISPONDENZA FRA CHIAVI E LEGITTIMO PROPRIETARIO)?***
- ***CHI GENERA LE CHIAVI?***

PER RENDERE FUNZIONANTE UN SISTEMA DI CRITTOGRAFIA A CHIAVE PUBBLICA OCCORRE DISPORRE DI

- ***UN SISTEMA DI CERTIFICAZIONE***
- ***UNA INFRASTRUTTURA RESPONSABILE DELLA GESTIONE DELLE CHIAVI E DEGLI ELENCHI PUBBLICI***

PER IL SISTEMA DI CERTIFICAZIONE CI SONO DUE SOLUZIONI ALTERNATIVE

- **ISTITUZIONE DI AUTORITÀ DI CERTIFICAZIONE (CA CERTIFICATION AUTHORITY) CHE AGISCONO DA GARANTI;**
- **APPROCCIO DECENTRATO DOVE GLI UTENTI SI CERTIFICANO RECIPROCAMENTE (PROGRAMMA PGP).**

LA NORMATIVA ITALIANA, SU SUGGERIMENTO DELL' AIPA (ORA CNIPA), HA ADOTTATO LA PRIMA SOLUZIONE.

PER LA GESTIONE DELLE CHIAVI ESISTONO DUE ORIENTAMENTI

- **LE CHIAVI VENGONO GENERATE DALLA PUBBLICA AMMINISTRAZIONE O DA UNA AUTORITÀ DI CERTIFICAZIONE**
- **LE CHIAVI VENGONO GENERATE DALL'UTENTE, CITTADINO ENTE O P.A., CHE POI CONSEGNA QUELLA PUBBLICA ALLA AUTORITÀ DI CERTIFICAZIONE**

LA PRIMA SOLUZIONE APPARE INACCETTABILE DAL PUNTO DI VISTA DELLA DEMOCRAZIA E DELLA TUTELA DELLA PRIVACY

NEL CASO CHE ESISTANO PIÙ AUTORITÀ DI CERTIFICAZIONE È NECESSARIA LA CREAZIONE DI UNA

***INFRASTRUTTURA DI CRITTOGRAFIA
A CHIAVE PUBBLICA (PKI)***

CHE SOVRINTENDA E REGOLI IL SISTEMA DAL PUNTO DI VISTA TECNICO E NORMATIVO.

LO STANDARD ISO X.509 PREVEDE UNA CATENA GERARCHICA NEL QUALE LE AUTORITÀ DI CERTIFICAZIONE SONO CONTROLLATE DA ALTRE AUTORITÀ DI LIVELLO SUPERIORE.

LA REGOLAMENTAZIONE E LA GESTIONE DI UNA INFRASTRUTTURA DI CRITTOGRAFIA A CHIAVE PUBBLICA È ESTREMAMENTE COMPLESSA E COINVOLGE DELICATI PROBLEMI RIFERITI ALLA DEMOCRAZIA E ALLA TUTELA DELLA PRIVACY DEI CITTADINI.

KEY RECOVERY CONSENTE ALLE AUTORITÀ DI VENIRE LEGALMENTE IN POSSESSO DELLA CHIAVE PRIVATA DI CIFRATURA

KEY ESCROW LE CHIAVI PRIVATE DI CIFRATURA SONO DEPOSITATE PRESSO UN TERZO

COSA SUCCEDE SE UNA CHIAVE PRIVATA VA PERDUTA?

KEY BACKUP SI ADOTTA UN MECCANISMO DI KEY ESCROW COSTITUENDO UN ORGANISMO FIDATO IL QUALE HA IN CONSEGNA COPIA DELLE CHIAVI;

LA SOLUZIONE DEL DOPPIO CIECO.

IL DOCUMENTO ELETTRONICO

LA DIZIONE PIÙ CORRETTA E' QUELLA DI **DOCUMENTO DIGITALE, IN QUANTO PIÙ GENERALE, COMPRENDENDO OLTRE LA FORMA ELETTRONICA, FRA LE ALTRE QUELLA MAGNETICA E QUELLA OTTICA.**

IL DOCUMENTO È LA RAPPRESENTAZIONE SENSIBILE DI UNA MANIFESTAZIONE DI VOLONTÀ DA PARTE DI CHI LO HA REDATTO.

NEL DOCUMENTO SI DISTINGUONO DUE PARTI FONDAMENTALI CHE LO COSTITUISCONO:

- ***IL SUPPORTO FISICO***
- ***IL CONTENUTO INFORMATIVO***

NELLA PRATICA DI OGNI GIORNO NON VI È DIFFERENZA FRA IL DOCUMENTO ED IL MEZZO FISICO CHE LO RAPPRESENTA (UN CONTRATTO È LA CARTA DA BOLLO SULLA QUALE È REDATTO, UNA LETTERA È IL FOGLIO SU CUI È SCRITTA ETC.).

FINO AD OGGI PER GARANTIRE L'AUTENTICITÀ DI UN DOCUMENTO BASTAVA GARANTIRE L'AUTENTICITÀ DEL SUO SUPPORTO MEDIANTE DEI MEZZI FISICI: APPOSIZIONE DI FIRMA AUTOGRAFA, TIMBRI SIGILLI ETC.

IL DOCUMENTO ELETTRONICO È "LA RAPPRESENTAZIONE INFORMATICA DI ATTI, FATTI O DATI GIURIDICAMENTE RILEVANTI".

LA VALIDITÀ DI UN DOCUMENTO ELETTRONICO, SOTTO CERTE CONDIZIONI, PRESCINDE DAL SUPPORTO FISICO CHE LO OSPITA RIMANENDO SEMPRE COPIA ORIGINALE ED AUTENTICA DI SE STESSO.

L 'INTRODUZIONE NELL'ORDINAMENTO GIURIDICO ITALIANO DELLA FATTISPECIE "DOCUMENTO INFORMATICO", ALL'INTERNO DEI PROVVEDIMENTI BASSANINI, HA UNA RILEVANZA ECCEZIONALE IN QUANTO PERMETTE LA COSTRUZIONE DI UNA INFRASTRUTTURA INFORMATICA IN GRADO DI RIDURRE QUASI A ZERO L'UTILIZZO DELLA CARTA NEI RAPPORTI FRA CITTADINI E P.A. ED ALL'INTERNO DI QUESTA

FIRMA DIGITALE

LA FIRMA DIGITALE È DI NATURA TOTALMENTE DIVERSA DA QUELLA "TRADIZIONALE" IN QUANTO ESSA NON ALTERA IL DOCUMENTO CUI SI RIFERISCE (NON VIENE AGGIUNTA AD ESSO)

LA FIRMA DIGITALE SI ASSOCIA AD UN DOCUMENTO INFORMATICO.

LA FIRMA DIGITALE È IL RISULTATO DI UN PROCEDIMENTO MATEMATICO APPLICATO AL CONTENUTO INFORMATIVO DEL DOCUMENTO.

CONSEGUENZE

- ***È PIÙ AFFIDABILE E SICURA DELLA TRADIZIONALE FIRMA AUTOGRAFA***
- ***SODDISFA ALLE PROBLEMATICHE DI SICUREZZA***

CARATTERI DELLA FIRMA DIGITALE

- ***È SEPARATA DAL DOCUMENTO CUI SI RIFERISCE, E NON LO MODIFICA IN ALCUN MODO***
- ***È DIVERSA DA UN DOCUMENTO AD UN ALTRO (DIPENDE DAL CONTENUTO DEL DOCUMENTO)***
- ***NON SI PUÒ APPORRE IN BIANCO (DEVE RIFERIRSI AD UN CONTENUTO)***

CARATTERI DELLA FIRMA DIGITALE

- ***PUÒ ESSERE VERIFICATA DA CHIUNQUE IN MODO CERTO E RIPETIBILE***
- ***RIVELA EVENTUALI MODIFICAZIONI DEL TESTO***
- ***NON PUÒ ESSERE RIPUDIATA (DISCONOSCIUTA)***

COME FUNZIONA LA FIRMA DIGITALE

PER REALIZZARE UN SISTEMA DI FIRMA DIGITALE SONO NECESSARI:

- ***LA DISPONIBILITÀ DI UNA FUNZIONE HASH***
- ***LA DISPONIBILITÀ DI UN SISTEMA DI CRITTOGRAFIA A CHIAVE PUBBLICA***

LA FUNZIONE HASH E' UNA ALGORITMO CHE APPLICATO AD UN DOCUMENTO DIGITALE GENERA UN NUMERO CHIAMATO *IMPRONTA*, DI LUNGHEZZA COSTANTE, CHE DIPENDE STRETTAMENTE DAL DOCUMENTO ORIGINARIO

LA FUNZIONE DI HASH GARANTISCE L'UNICITÀ DELL'IMPRONTA

LA FUNZIONE DI HASH NON È (È DIFFICILMENTE) INVERTIBILE

Siano

$h(x)$ UNA FUNZIONE DI HASH

A UTENTE POSSESSORE DI UNA COPPIA DI CHIAVI CRITTOGRAFICHE

d DOCUMENTO DA FIRMARE

1. LA FUNZIONE DI HASH CALCOLA L'IMPRONTA DI d

$$d' = h(d)$$

2. SI CIFRA L'IMPRONTA d' CON LA CHIAVE INVERSA (DI DECIFRATURA) DI A OTTENENDO LA FIRMA DIGITALE DI A ASSOCIATA AL DOCUMENTO d