Alessandra ARDISSONE – TSS 2019

LA SICUREZZA NELLE COMUNICAZIONI TELEMATICHE

Due dei primi problemi che emergono quando si invia o si riceve un documento informatico per via telematica, quale è un messaggio di **posta elettronica**, sono:

1. poter avere la **certezza** che esso sia **autentico**, privo cioè di contraffazioni e **integro** dal momento dell'invio alla ricezione da parte del destinatario;
2. assicurarsi che tale messaggio possa essere **letto esclusivamente dal destinatario** a cui in origine è indirizzato.

Per poter ovviare a questi problemi si è ideato un sistema di cifratura chiamato **crittografia asimmetrica**.

LA CRITTOGRAFIA

La crittografia è una tecnica di rappresentazione di un messaggio in una forma tale che l'informazione in esso contenuta possa essere recepita **solo dal destinatario**; essa viene attuata con metodi che "trasformano" il testo/contenuto del messaggio rendendolo incomprensibile a chiunque eccetto che al destinatario stesso, che possiede la "**chiave**" per poterlo decifrare.

In crittografia una **chiave** è un'informazione usata come parametro in un **algoritmo crittografico**[1]. Le chiavi sono utilizzate in molte applicazioni crittografiche e, secondo il **principio di Kerckhoffs**[2], sono l'**unico dato** che è davvero necessario tenere **segreto**. La **dimensione** della chiave, generalmente misurata in **bit**, dipende dal particolare algoritmo usato: alcuni algoritmi possono utilizzare chiavi di lunghezze diverse e in questo caso più lunga è la chiave tanto più difficile sarà forzare il messaggio cifrato.

Nell'informatica la crittografia si implementa principalmente con l'utilizzo della **firma digitale**.

LA FIRMA DIGITALE

La firma digitale si compone, **fisicamente**, di un **supporto elettronico** (solitamente un **chip** integrato in una card di materiale plastico) che può essere letto da un apposito lettore previo l'inserimento, da parte del proprietario della firma, di un **PIN** (codice di quattro o più cifre) di

1 Un algoritmo è un procedimento che risolve un determinato problema attraverso un numero finito di passi elementari, chiari e non ambigui, in un tempo ragionevole.

2 In crittografia, il **principio di Kerckhoffs** (conosciuto anche come assunzione, assioma o legge di Kerckhoffs), fu enunciato dal crittografo olandese Auguste Kerckhoffs alla fine del 1880. Esso afferma che la sicurezza di un crittosistema non deve dipendere dal tenere celato il crittoalgoritmo ma solo dal **tenere celata la chiave**. In altre parole, il sistema deve rimanere sicuro anche nell'ipotesi che il nemico conosca l'algoritmo di crittazione. Quest'ultimo può anche essere di pubblico dominio; l'unica cosa che importa è che rimanga segreta la chiave. Il principio è stato riformulato (o forse indipendentemente formulato) da **Claude Shannon** nella forma "**il nemico conosce il sistema**": "un sistema dovrebbe essere progettato sotto l'assunzione che il nemico guadagnerà immediatamente familiarità con esso". In questa forma, il principio è noto come **massima di Shannon**.

abilitazione. Un documento sottoscritto con firma digitale **certifica in modo assoluto l'identità del firmatario**; attesta inoltre, che quel file/messaggio **non è stato in alcun modo modificato** dopo essere stato firmato; infine, il documento informatico sottoscritto con firma digitale è **valido a tutti gli effetti dal punto di vista legale** e **non può essere ripudiato** dal firmatario.

In **Italia** attualmente la firma digitale può essere richiesta esclusivamente presso i **Certificatori autorizzati dal Governo**, per cui i cittadini, le aziende e le Pubbliche Amministrazioni che intendono richiederla si devono necessariamente rivolgere ai Certificatori presenti nell'**Elenco pubblico dei Certificatori di firma digitale** disponibile online sul sito istituzionale dell'**AgID** (ex DigitPA), l'ente nazionale per la digitalizzazione della Pubblica Amministrazione, all'indirizzo: https://dss.agid.gov.it/tsl-info/it.

La firma digitale funziona come una vera e propria firma tradizionale che serve a garantire che un determinato documento inviato online sia certificato nella sua integrità e autenticità. Per svolgere queste funzioni di **sicurezza**, occorre che la firma digitale sia **generata** attraverso il cosiddetto metodo chiamato "**crittografia a doppia chiave**", ossia una firma ottenuta dal connubio di **due chiavi, privata e pubblica**.

Pertanto, quando un documento viene inviato dall'utente con la firma digitale, questo è firmato con la **chiave privata** che il sistema di certificazione riconosce e trasforma nella corrispondente **chiave pubblica**.

La firma digitale è quindi generata da una **coppia di chiavi digitali asimmetriche**, attribuite in maniera **univoca** ad un soggetto, chiamato **titolare della coppia di chiavi**:

- **Chiave privata**: è la chiave utilizzata per la **generazione** della firma digitale da apporre al documento ed è **conosciuta solo dal titolare**;
- **Chiave pubblica**: utilizzata per **verificare l'autenticità** della firma mediante specifici software di controllo ed è disponibile per chiunque.

CRITTOGRAFIA A DOPPIA CHIAVE O CRITTOGRAFIA ASIMMETRICA

La **crittografia asimmetrica**, conosciuta anche come **crittografia a coppia di chiavi**, **crittografia a chiave pubblica/privata** o anche solo **crittografia a chiave pubblica**, è un tipo di crittografia dove, come si evince dal nome, ad **ogni attore** coinvolto nella comunicazione è associata una **coppia di chiavi**:

- la **chiave pubblica**, che deve essere **distribuita**;
- la **chiave privata**, appunto **personale** e **segreta**;

evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica. Il meccanismo si basa sul fatto che, **se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra**.

Ci sono **due funzioni** che possono essere realizzate: **cifrare** messaggi con la chiave **pubblica** per garantire che solo il **titolare** della chiave **privata** possa **decifrarlo** oppure usare la chiave **pubblica** per **autenticare** un messaggio inviato dal titolare con la chiave **privata abbinata**.

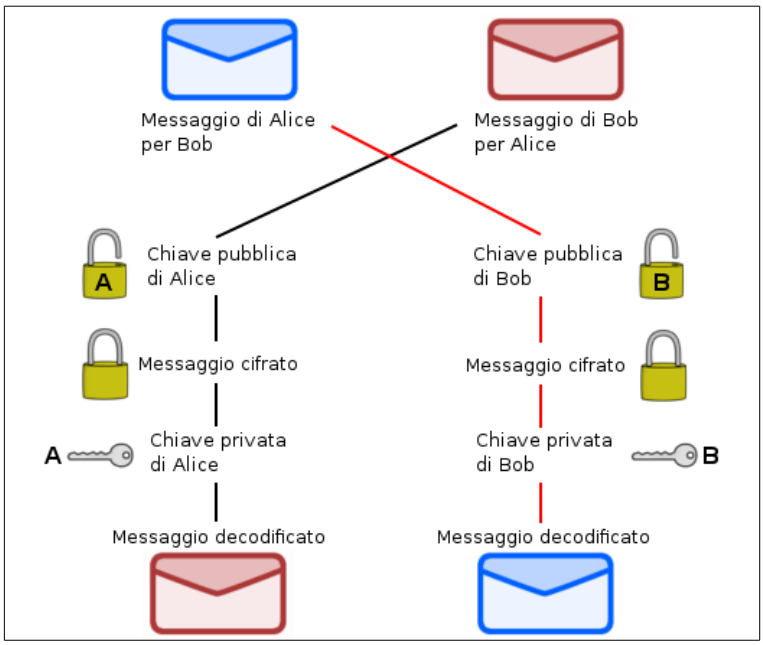
In un sistema di crittografia a chiave pubblica, **chiunque può cifrare** un messaggio usando la chiave **pubblica** del **destinatario**, ma tale messaggio può essere **decifrato solo** con la chiave **privata** del destinatario. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica.

La **sicurezza** dipende quindi solo dal mantenere la **chiave privata segreta**, mentre la **chiave pubblica** può essere per l'appunto **pubblicata** senza compromettere la sicurezza.

COME FUNZIONA: ALICE E BOB

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il **mittente** è **Alice** ed il **destinatario Bob**, i **lucchetti** fanno le veci delle chiavi **pubbliche** e le **chiavi** recitano la parte delle chiavi **private**:

- **Alice** chiede a Bob di spedirle il **lucchetto** già **aperto**. La **chiave** dello stesso verrà però gelosamente conservata da **Bob**;
- **Alice** riceve il **lucchetto** di Bob e, con esso, **chiude** il pacco e lo spedisce a Bob;
- **Bob** riceve il pacco e può **aprirlo con la chiave** di cui è l'**unico** proprietario;
- Se adesso **Bob** volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il **lucchetto** di **Alice** (che lei dovrebbe aver preventivamente dato a Bob) che solo lei potrebbe aprire.



Si può notare come per mettere in **sicurezza** il contenuto dei pacchi ci sia bisogno del **lucchetto del destinatario**, mentre per **aprirli** viene usata esclusivamente la **propria chiave segreta**, rendendo l'intero processo di cifratura/decifratura asimmetrico (una chiave per cifrare ed una differente per decifrare). Chiunque intercettasse il lucchetto (aperto) o il messaggio chiuso con il lucchetto non potrebbe leggerne il contenuto poiché non ha la chiave. Uno dei **vantaggi** della crittografia asimmetrica sta nel fatto che le **chiavi pubbliche** possono essere **scambiate** anche utilizzando un **mezzo insicuro, come Internet**.

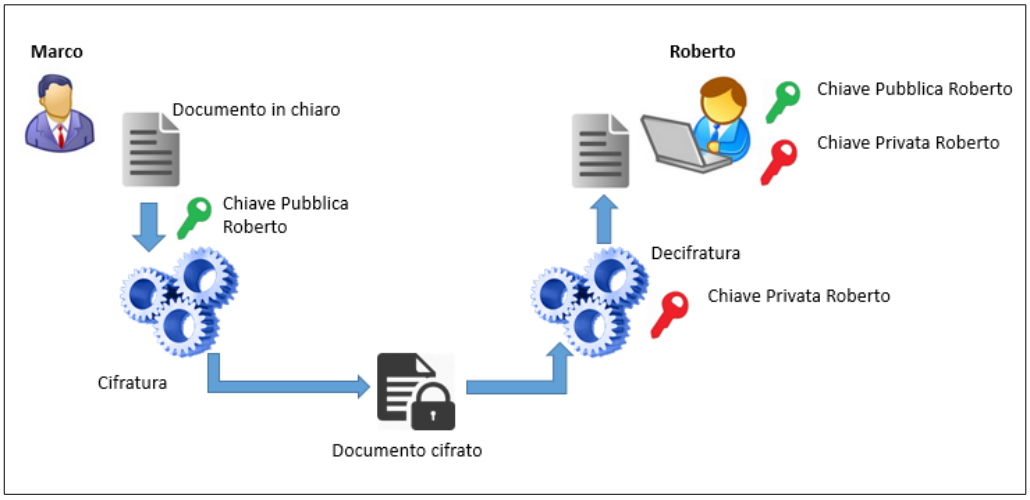
Usando un'altra similitudine, si può dire che il metodo è analogo a quello di una cassaforte che abbia due chiavi distinte, una usata per aprirla (chiave segreta), l'altra per chiuderla (chiave pubblica).

Nella crittografia **simmetrica** invece, che basa la sicurezza del sistema sulla **segretezza della chiave di codifica/decodifica** utilizzata, si rende necessario utilizzare un **canale sicuro** per la trasmissione della chiave, poiché l'intercettazione della stessa, da parte di terzi, vanificherebbe la sicurezza del sistema stesso.

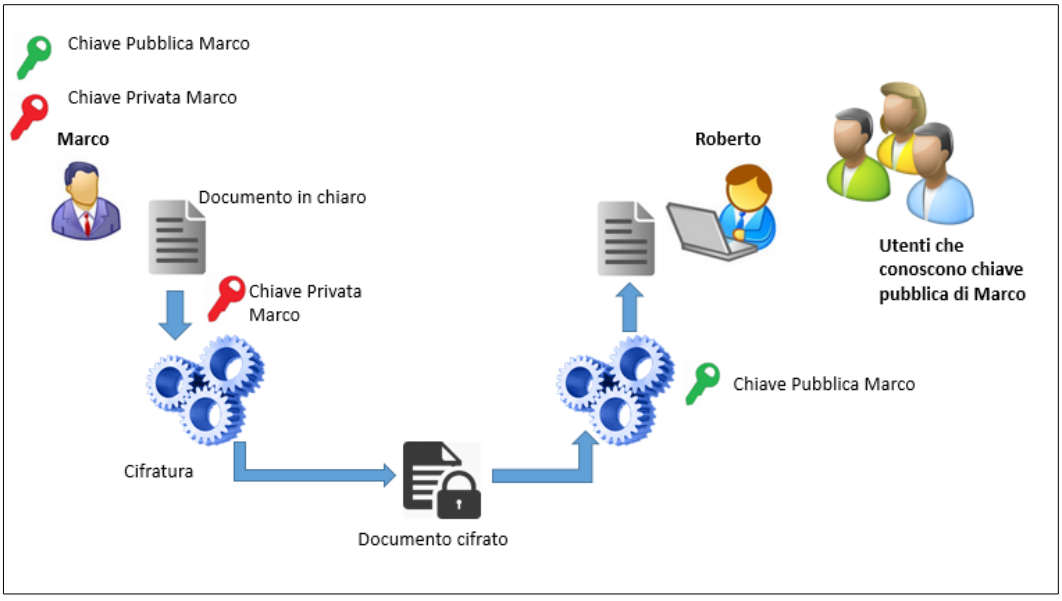
Due degli usi più conosciuti della **crittografia asimmetrica** sono:

- **crittografia a chiave pubblica**, nel quale i messaggi sono crittografati con la chiave pubblica del destinatario. Il messaggio non può essere decriptato da chi non possiede la chiave privata corrispondente, che viene così presupposto di essere il proprietario di quella chiave

e la persona associata con la chiave pubblica. Questo è utilizzato nel tentativo di **garantire la riservatezza**;



- **firma digitale**, come già illustrato sopra, in cui un messaggio viene firmato con la chiave privata del mittente e può essere verificato da chiunque abbia accesso alla chiave pubblica del mittente. Questa verifica dimostra che il **mittente** ha avuto accesso alla chiave privata ed è pertanto probabile che sia la **persona associata** alla chiave pubblica, il che **garantisce l'autenticazione del mittente**. Questo assicura anche che il **messaggio non è stato manomesso**.



PROBLEMATICHE

Il problema della **sicurezza** riguardante la **segretezza** della comunicazione non è del tutto risolto con questo tipo di crittografia, in quanto passibile di attacchi di tipo **man in the middle**[3]: non si può essere certi infatti che la chiave appartenga davvero alla persona nominata

3 **Attacco man in the middle** (spesso abbreviato in MITM, MIM, MIM attack o MITMA, in italiano "uomo nel mezzo") è una terminologia usata per indicare un **attacco informatico** in cui qualcuno segretamente **ritrasmette o altera** la comunicazione tra due parti che credono di comunicare direttamente tra di loro.

nell'intestazione della chiave stessa, risultando quindi sensibili ad attacchi di tipo **spoofing**[4] (furto di identità) in assenza di un meccanismo di autenticazione tra le parti in causa. Una **soluzione** resta sempre il **contatto fisico** tra i due interlocutori, i quali, scambiandosi le chiavi pubbliche, hanno una reciproca autenticazione.

Un altro problema da non escludere è quello dell'**effettiva protezione della chiave privata**: quando questa, ad esempio, risiede nel disco rigido del proprietario ed è generalmente cifrata con una password (quindi con crittografia simmetrica), data la relativa semplicità di accesso (basta inserire una password per "sbloccarla"), con particolari **trojan/keylogger** programmati ad-hoc è possibile ricavare dal PC della vittima sia il file contenente la chiave privata sia la password per utilizzarla, violando a tutti gli effetti l'efficienza della crittografia asimmetrica.

Nel caso in cui, come spiegato in precedenza a proposito della firma digitale, la chiave privata sia contenuta in una **smart-card protetta da codice PIN**, il proprietario deve pertanto avere la **massima cura nella custodia e della chiave e del codice di sblocco**, che ovviamente vanno conservati in luoghi **separati**.

FONTI

- GUIDAFISCO.IT - Firma Digitale: cos'è e come funziona, come richiederla e costi 2019: https://www.guidafisco.it/firma-digitale-aruba-poste-camera-commercio-1015
- AgendaDigitale.eu - Firma digitale: cos'è, come funziona e come ottenerla: https://www.agendadigitale.eu/documenti/firma-digitale-cose-come-funziona-e-come-ottenerla
- Namirial S.p.A. Trust Service Provider - Definizione Firma Digitale: https://www.firmacerta.it/firma-digitale-info.php
- BUCAP.it - Definizione e impiego della crittografia asimmetrica: https://www.bucap.it/news/approfondimenti-tematici/firma-digitale/definizione-impiego-della-crittografia-asimmetrica.htm
- Bit4id.com - Crittografia Asimmetrica… come, quando e perché: http://www.firmadigitalefacile.it/crittografia-asimmetrica-come-quando-e-perche
- Wikipedia – Crittografia e voci correlate: https://it.wikipedia.org/wiki/Crittografia

QUIZ RIASSUNTIVO

1. Il non ripudio è uno degli obiettivi della sicurezza informatica che riguarda:
   A) La possibilità di identificare in modo certo e univoco chi legge i dati.
   B) La possibilità di garantire che i dati non vengano manipolati.
   C) La possibilità di fornire una prova formale che dimostri, come una firma, che una certa persona ha sottoscritto un messaggio.
   D) La possibilità di verificare che un certo dato non è stato letto senza autorizzazione.

4 Lo **spoofing** è un tipo di **attacco** informatico che impiega in varie maniere la **falsificazione dell'identità** (spoof). Lo spoofing può avvenire a **qualunque livello della pila ISO/OSI** e può riguardare anche la falsificazione delle informazioni applicative.

2. Se A vuole mandare a B un messaggio riservato che solo B possa leggere, deve criptarlo:
   A) Con la chiave pubblica di B.
   B) Con la chiave pubblica di A.
   C) Con la chiave privata di B.
   D) Con la chiave privata di A.

3. Se A vuole mandare a B un messaggio autenticandolo in modo che B sia certo della provenienza del messaggio deve criptarlo:
   A) Con la chiave pubblica di B.
   B) Con la chiave pubblica di A.
   C) Con la chiave privata di B.
   D) Con la chiave privata di A.

4. Se A invia a B un documento cifrato con la propria chiave pubblica:
   A) B deve decifrare il documento con la propria chiave privata.
   B) B deve decifrare il documento con la chiave privata di A.
   C) A deve ulteriormente cifrare il documento con la propria chiave privata.
   D) A ha sbagliato ad inviare il documento.

5. Se B vuole garantire ad A che è stato lui e solo lui a inviare il documento:
   A) Lo cifra con la propria chiave pubblica.
   B) Lo cifra con la propria chiave privata.
   C) Lo decifra con la chiave pubblica di A.
   D) lo cifra con la chiave pubblica di A.

SOLUZIONI

1. C
2. A
3. D
4. D
5. B