

Materiale didattico
validato da AICA
Certificazione EUCIP
IT Administrator
Modulo 5 -
IT Security
Sicurezza informatica



"AICA Licenziataria esclusiva in Italia del programma EUCIP (European Certification of Informatic Professionals), attesta che il materiale didattico validato copre puntualmente e integralmente gli argomenti previsti nel Syllabus IT Administrator e necessari per il conseguimento della certificazione IT Administrator IT Security. Di conseguenza AICA autorizza sul presente materiale didattico l'uso del marchio EUCIP, registrato da EUCIP Ltd e protetto dalle leggi vigenti"

Riferimento Syllabus 2.0 (curriculum ufficiale AICA)

5.2.1. Concetti generali

5.2.1.1 Basi della crittografia

► Concetti e algoritmi di crittografia

Scopriamo i fondamenti e le tecniche di crittografia

Prosegue il primo corso di taglio professionale destinato al conseguimento della certificazione ufficiale, EUCIP IT Administrator – Sicurezza Informatica, valida in tutta Europa. La seconda lezione esplora tutti i principali algoritmi e standard di crittografia utilizzati per garantire riservatezza, l'integrità e l'autenticità dei documenti. Anche in questo caso i contenuti si articolano in tre elementi: un articolo sulla rivista, un articolo, molto più esteso in formato PDF e un corso multimediale completo su CD e DVD di [Giorgio Gobbi](#)

Obiettivo del corso IT Administrator Sicurezza Informatica

Fornire al lettore familiarità con i vari modi di proteggere i dati sia su un singolo PC sia in una LAN connessa a Internet. In particolare, metterlo nelle condizioni di proteggere i dati aziendali contro perdite, attacchi virali e intrusioni. Inoltre, metterlo nelle condizioni di conoscere e utilizzare le utility e i programmi più comuni destinati a tali scopi.

Le reti di computer, soprattutto attraverso Internet, hanno reso possibile la rapida e facile comunicazione tra utenti oltre che tra aziende e compratori. Con 285 milioni di siti attivi (ottobre 2004) e oltre 800 milioni di utenti (febbraio 2005), gli scambi commerciali e le transazioni economiche che avvengono su Internet hanno raggiunto un volume ingente e sono in forte crescita, favoriti dalla progressiva fiducia nella sicurezza delle operazioni.

L'assenza del contatto personale e dello scambio di documenti cartacei intestati e firmati, richiede strumenti sostitutivi per identificare gli interlocutori, per mantenere la riservatezza e l'integrità delle informazioni scambiate e per conferire validità legale alla transazione, in modo che non possa essere disconosciuta (oppure, come si suol dire, ripudiata) dalla parte che contrae l'impegno (o in generale da tutte le parti in gioco).

In pratica, gli strumenti e le procedure della sicurezza informatica hanno il compito di fornire agli utenti (individui e organizzazioni) lo stesso livello di fiducia che provano quando eseguono lo stesso tipo di operazioni con i metodi tradizionali e le firme autografe. Nella lezione precedente abbiamo trattato dell'analisi del rischio, una fase essenziale del programma di sicurezza, dove si considerano le probabilità di attuazione delle minacce e la gravità del loro impatto per selezionare le contromisure da mettere in campo. Si tratta di un approccio fondamentalmente difensivo o passivo, che valuta quali rischi accettare, quali delegare a terzi e quali controllare, riducendoli o azzerandoli.

Nella presente lezione ci occupiamo invece di sicurezza attiva, ossia delle misure di sicurezza che proteggono le informazioni in modo proattivo, in modo cioè da anticipa-

re e neutralizzare i problemi futuri. Questo viene ottenuto non solo impedendo agli estranei di accedere alle informazioni (sicurezza passiva o difensiva), ma rendendo le informazioni intrinsecamente sicure a livello applicativo, proteggendone la riservatezza (confidentiality, chiamata anche confidenzialità), l'integrità e l'autenticità. Vedremo che le tecniche crittografiche permettono 1) di trasformare dati, informazioni e messaggi in modo da nascondere il contenuto a chiunque non sia autorizzato e attrezzato per prenderne visione, 2) di impedire a estranei di alterare i dati, segnalando qualunque tentativo in tal senso e 3) di garantire l'autenticità dei dati, associandoli in modo certo al loro proprietario, impedendo allo stesso tempo che il mittente di un messaggio possa ripudiare la paternità.

I contenuti delle 8 lezioni

Lezione 1: Informazioni generali

Lezione 2: parte 1 Crittografia - fondamenti e algoritmi

Lezione 2: parte 2 Crittografia - applicazioni

Lezione 3: Autenticazione e controllo degli accessi

Lezione 4: Disponibilità

Lezione 5: Codice maligno

Lezione 6: Infrastruttura a chiave pubblica

Lezione 7: Sicurezza della rete

Lezione 8: Aspetti sociali, etici e legali della sicurezza informatica

In collaborazione con:



IT Administrator comprende sei moduli:

- 1 Hardware del PC (PC Hardware)
- 2 Sistemi operativi (Operating Systems)
- 3 Reti locali e servizi di rete (LAN and Network Services)
- 4 Uso esperto delle reti (Network Expert Use)
- 5 Sicurezza informatica (IT Security)
- 6 Progettazione reti (Network Design)

L'argomento di questo corso è il modulo 5 della certificazione EUCIP IT Administrator, dedicato espressamente alla sicurezza informatica. Il modulo 5 garantisce comunque il diritto a una certificazione a sé stante.

Sul CD Guida 3 e sul DVD trovate un articolo che spiega il modo per ottenere la certificazione.

Per meglio apprezzare i vantaggi della sicurezza attiva, proviamo a immaginare cosa accadrebbe a un messaggio confidenziale che venisse inviato su Internet. Sul computer di partenza, il messaggio, contenuto nell'archivio della posta elettronica, sarebbe leggibile da chiunque si procurasse l'accesso al computer, un'operazione relativamente facile dall'interno dell'organizzazione e non impossibile dall'esterno se mancano le opportune difese. Nel momento in cui il messaggio viene spedito, attraversa la rete locale interna (dove può essere intercettato tramite analizzatori di rete, packet sniffer e altri strumenti per intercettare i pacchetti), esce dall'edificio, raggiunge la centrale del gestore di telecomunicazioni, viene instradato verso il sito che ospita il server di e-mail e qui staziona in una casella postale in attesa di essere prelevato. Una volta prelevato, secondo i casi, viene cancellato o meno dal server e viene comunque trasferito sul computer del destinatario, nell'archivio personale di posta elettronica. Durante il percorso, il messaggio è intercettabile dagli organismi di sicurezza nazionali (di solito su mandato della magistratura) e, se fosse per qualche verso appetibile, anche da agenzie di sicurezza che non chiedono permessi. Inoltre, se il messaggio contenesse informazioni preziose per nemici, concorrenti e specialisti di furto e ricatto, lungo il suo percorso, dal computer di origine a quello di destinazione, potrebbe trovare in agguato hacker, dispositivi di rilevamento o individui che, mediante tecniche di social engineering, si procurano i file da chi ha o può procurare (anche inconsapevolmente) il diritto di accesso. Il social engineering, nel campo della sicurezza informatica, è la pratica di manipolare ad arte le persone per indurle a compiere azioni (come l'esecuzione di software maligno) oppure a rivelare informazioni (come le password) utili a ottenere accesso a dati e risorse. Si comprende la complementarità della difesa passiva e di quella attiva con un esempio. Supponiamo che su un computer siano installati sistemi crittografici che proteggono i documenti dal momento in cui sono archiviati localmente in poi (trasmissione, prelievo dal mail server e archiviazione sul computer di destinazione). Supponiamo al tempo stesso che, per carenza di sicurezza difensiva, un malintenzionato convinca l'utente a eseguire un'applicazione particolarmente interessante o divertente, che in realtà installa un key logger, cioè un registratore dell'input di tastiera, salvato in un file che potrà essere prelevato segretamente attraverso Internet, anche tramite e-mail. In questo scenario, i documenti sono crittografati e ben protetti come tali, ma il loro contenuto è stato intercettato a monte e viene trasmesso all'esterno.

La crittografia

La parola crittografia deriva dal greco *kryptós* (nasco-

sto) e *graphein* (scrivere). L'utilizzo della "scrittura nascosta", come accennato nella prima lezione, risponde da millenni all'esigenza di mantenere riservate o segrete certe categorie di comunicazioni, a partire da quelle militari. La crittografia non studia come nascondere un messaggio (di cui si occupano altre tecniche, come la steganografia – che deriva dal greco *stèganos* – rendo occulto, nascondo), bensì come nascondere il significato o contenuto di un messaggio (o di un documento) in modo che risulti comprensibile solo al destinatario stabilito dal mittente.

Il mittente di un messaggio prende il testo originale, detto testo in chiaro, lo sottopone a un'operazione di cifratura e ottiene il testo cifrato. Il destinatario esegue un'operazione di decifratura per ricostruire il messaggio originale. Per semplicità, e per assonanza con i termini in lingua inglese (*plaintext* e *ciphertext*), parliamo spesso di testo, intendendo che documenti e messaggi possono contenere anche immagini, sequenze audio/video, dati binari eccetera.

Il metodo utilizzato per cifrare il messaggio è detto algoritmo di crittografia o cifrario.



Un esempio di algoritmo è la sostituzione di ogni lettera con la lettera che si trova tre posizioni più avanti nell'alfabeto ed è noto come cifrario di Cesare. Nella moderna crittografia un cifrario prevede l'uso di una chiave di cifratura, una sequenza di caratteri di lunghezza massima stabilita che governa il funzionamento dell'algoritmo. L'algoritmo esegue una serie di trasformazioni dal testo in chiaro al testo cifrato: la chiave determina l'entità delle sostituzioni, trasposizioni e altre operazioni che formano l'algoritmo, così che, al variare della chiave, cambia il testo cifrato. Idealmente, per un dato testo in chiaro e per un dato algoritmo di cifratura, chiavi diverse generano sempre testi cifrati diversi.

L'algoritmo definisce anche le regole con cui il testo cifrato viene ritrasformato nel testo in chiaro originale attraverso l'uso di una chiave di decifratura.

I moderni standard di crittografia si ispirano al Principio di Kerchoff. Nel 1883, Auguste Kerchoff pubblicò un articolo in cui sosteneva che l'unico aspetto segreto di un sistema crittografico dovrebbe essere la chiave. Kerchoff affermava che l'algoritmo dovrebbe essere di pubblico dominio e che un sistema di sicurezza basato su troppi segreti finisce con l'essere più vulnerabile. Questo punto di vista è condiviso dal settore privato, ma non necessariamente dalle agenzie militari e governative, che amano creare i propri algoritmi mantenendoli segreti. Viceversa, è solo rendendo gli algoritmi ben noti che se ne possono scoprire le eventuali debolezze e vulnerabilità e si possono confrontare le caratteristiche delle diverse soluzioni disponibili, inventando una nuova generazione di cifrari quando cominciano ad apparire le prime crepe in quelli consolidati.

Secondo il grado di sicurezza che si desidera ottenere, esistono diversi algoritmi e diverse gestioni delle chiavi. La lunghezza delle chiavi determina il numero di valori possibili (che raddoppia a ogni bit aggiunto) e lo sforzo necessario per ricostruire il messaggio in chiaro in assenza della chiave. La lunghezza della chiave non è un termine di paragone assoluto: secondo il tipo di algoritmo, varia la lun-



L'elemento centrale della crittografia è il cifrario o algoritmo di cifratura che permette la trasformazione del contenuto di un messaggio in modo che non sia leggibile da estranei

Il documento cifrato può essere ricostruito solo da chi possiede il cifrario adatto.

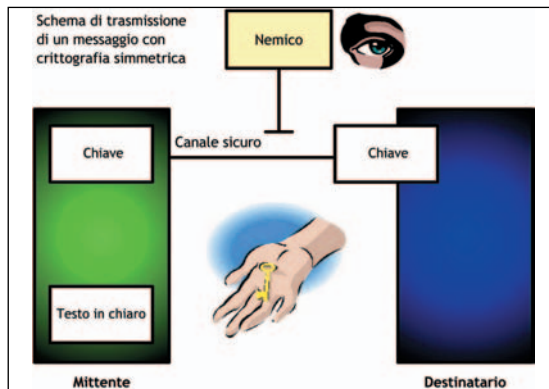
Nella cifratura simmetrica la chiave è unica e viene condivisa da mittente e destinatario, perciò va mantenuta segreta. Per tale motivo prende il nome di cifratura a chiave segreta

La cifratura simmetrica prevede l'uso di una chiave identica per cifrare e decifrare, perciò tale chiave va scambiata in modo sicuro

5.2.2 Crittografia simmetrica

5.2.2.1 Conoscere i principi della crittografia simmetrica

ghezza di chiave considerata sicura nel contesto tecnologico corrente.



Quando la chiave di cifratura è la stessa usata per la decifratura, o possono essere derivate facilmente una dall'altra, si parla di crittografia simmetrica. In questo caso, sia il mittente sia il destinatario concordano sull'algoritmo da utilizzare e sulla chiave segreta. Quest'ultima dovrà essere comunicata in modo sicuro (possibilmente di persona), dovrà essere mantenuta segreta (possibilmente affidata solo alla memoria) e dovrà essere cambiata spesso per evitarne la scoperta, vuoi per mancanza di riservatezza nel suo uso vuoi per via matematico-statistica analizzando un vasto campione di messaggi.

Se la chiave di cifratura è diversa da quella di decifratura, si parla di crittografia asimmetrica. In tal caso le due chiavi sono generate contestualmente; una di esse prende il nome di chiave privata ed è tenuta segreta (e custodita al sicuro) dal proprietario, mentre l'altra, detta chiave pubblica, può essere messa a disposizione di chiunque. Le caratteristiche principali di questa coppia di chiavi sono le seguenti:

1) per ogni chiave pubblica esiste una sola chiave privata e viceversa, 2) se si utilizzano chiavi abbastanza grandi, non è praticamente possibile ricavare la chiave privata dalla chiave pubblica, 3) per cifrare un documento si può usare sia la chiave privata sia la chiave pubblica; per la decifratura si deve usare l'altra chiave della coppia.

Se per esempio si cifra un messaggio con la chiave pubblica del destinatario, solo quest'ultimo sarà in grado di decifrarlo, utilizzando la corrispondente chiave privata. Se invece si cifra un messaggio con la propria chiave privata e si rende disponibile la chiave pubblica, chiunque potrà decifrarlo (a patto di conoscere l'algoritmo utilizzato e di procurarsi la chiave pubblica). Mentre un messaggio cifrato con una chiave pubblica non garantisce l'identità del mittente e l'integrità del messaggio (chiunque può usare una chiave pubblica), un messaggio cifrato con una chiave privata, nel momento in cui viene decifrato con la chiave pubblica, assicura che proviene dal proprietario delle chiavi e che non è stato modificato lungo il percorso. Su questo principio si basa la firma digitale, di cui parleremo più avanti.

Obiettivi della sicurezza attiva

Abbiamo introdotto il concetto di sicurezza attiva, complementare alle misure difensive della sicurezza passiva, per rendere i dati intrinsecamente sicuri. I servizi di sicurezza attiva, che proteggono dati e messaggi nei sistemi informatici e di comunicazione, hanno i seguenti obiettivi: riservatezza (o confidenzialità), privacy, integrità, autenticità e non ripudio.

I servizi di sicurezza che permettono di raggiungere questi obiettivi sono basati su tecniche crittografiche e, come è facile immaginare, fanno uso di architetture standardizzate e ben collaudate, di cui, almeno per il settore non mi-

litare, si conoscono in dettaglio le proprietà e il grado di sicurezza e affidabilità. L'accento è sull'uso di metodi e tecnologie che hanno raccolto ampio consenso per la loro efficacia ed efficienza e che permettono la facile interoperabilità delle applicazioni, evitando i rischi e le complessità delle soluzioni ad-hoc. Tutti gli obiettivi di sicurezza attiva citati sono ottenibili tramite tecniche crittografiche standardizzate.

Crittografia simmetrica

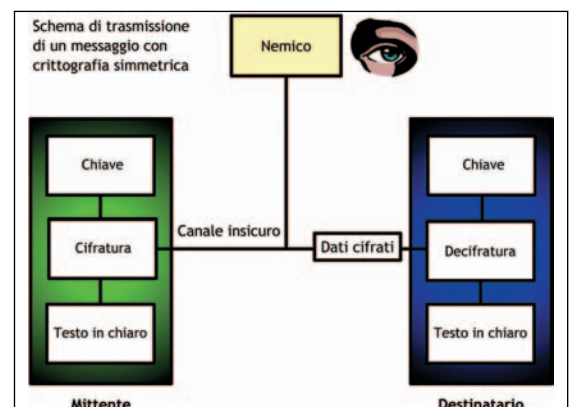
La crittografia simmetrica, detta anche crittografia a chiave segreta, richiede che i due interlocutori usino lo stesso algoritmo e la stessa chiave segreta. Ciò significa che si deve trovare un canale sicuro per consegnare al destinatario la chiave o, meglio, dati privi di valore intrinseco da cui il destinatario ricostruisca la chiave. Visto che ogni coppia d'interlocutori richiede una chiave segreta, se questa fosse un elemento statico, per esempio una frase concordata a voce tra due persone, il numero di chiavi da conservare crescerebbe esponenzialmente con il numero degli interlocutori. Per esempio, per proteggere la comunicazione tra 10 persone, sarebbero necessarie 45 chiavi, che crescono a quasi mezzo milione per 1.000 interlocutori. In generale, per N persone che scambiano messaggi cifrati con crittografia simmetrica, occorrono $N(N-1)/2$ chiavi e ciascuno degli N utenti deve conservare al sicuro N-1 chiavi. Di conseguenza, nella pratica si usano sistemi automatici per la generazione e lo scambio sicuro delle chiavi.

Un altro aspetto della crittografia simmetrica è che conferisce riservatezza al messaggio, ma non assicura l'autenticazione o il non ripudio, poiché non c'è un'associazione univoca e sicura tra la chiave e un individuo. Di conseguenza, il mittente apparente di un messaggio cifrato con chiave simmetrica potrebbe sempre negare di avere spedito il messaggio, attribuendone la responsabilità diretta o indiretta al destinatario (detentore della stessa chiave).

D'altra parte, gli algoritmi di crittografia simmetrica sono molto veloci da eseguire e difficili da violare, se la chiave è abbastanza lunga. La crittografia simmetrica è l'unica opzione utilizzabile per cifrare grandi quantità di dati, un'operazione fuori della portata degli algoritmi asimmetrici.

A un buon algoritmo di crittografia simmetrica sono richieste alcune proprietà fondamentali, in modo che l'analisi delle relazioni tra input e output non fornisca indicazioni sull'algoritmo o sulla chiave:

1) il testo cifrato dev'essere funzione di tutti i bit della chiave e del testo in chiaro, 2) non ci dev'essere nessuna relazione statistica evidente tra testo in chiaro e testo cifrato, 3) modificando un singolo bit nel testo o nella chiave, ogni bit del testo cifrato è soggetto alla stessa probabilità di variazione, 4) modificando un bit nel testo cifrato, ogni bit del testo decifrato è soggetto alla stessa probabilità di variazione.



I dati sono decifrabili solo da chi possiede la chiave anche se vengono trasmessi su un canale insicuro (accessibile ad estranei)

Esistono due tipi di cifrari simmetrici: a blocchi (block cipher) e a flusso (stream cipher).

I cifrari a blocchi operano sui dati un blocco alla volta (le dimensioni tipiche dei blocchi sono di 64 o 128 bit) e ogni operazione su un blocco è un'azione elementare. I cifrari a flusso operano invece un bit o un byte alla volta; una volta inizializzati con una chiave, producono un flusso di bit e si prestano alla cifratura di grandi quantità di dati.

I cifrari a blocchi possono operare in diversi modi, che in molti casi prevedono il concatenamento dei blocchi fornendo in input all'operazione corrente i risultati delle operazioni precedenti; il che rende il cifrario meno vulnerabile a certi tipi di attacchi.

I principali tipi di cifrari a blocchi sono due: ECB (Electronic Code Book), CBC (Cipher Block Chaining).

Alla base troviamo la modalità ECB: ogni blocco di testo in chiaro viene trasformato in un blocco di testo cifrato. Lo stesso blocco di testo, con la stessa chiave, produce sempre lo stesso blocco di testo cifrato, il che consente ai malintenzionati di compilare un codice (code book) di tutti i possibili testi cifrati corrispondenti a un dato testo in chiaro. Se per esempio sappiamo che il blocco di testo contiene un pacchetto IP (Internet Protocol), i primi 20 byte di testo cifrato rappresentano sicuramente l'intestazione IP del pacchetto e possiamo usare tale conoscenza, abbinata a un code book, per determinare la chiave. Al fine di avere blocchi di input di lunghezza stabilita dal cifrario, può essere necessario aggiungere all'input un riempitivo (padding).

Il fatto che ogni blocco è indipendente dagli altri e produce sempre lo stesso blocco cifrato, rende meno sicuro l'algoritmo e permette a un attaccante di sostituire un blocco con un altro senza che il fatto sia rilevato. Avendo a disposizione una quantità di dati sufficienti e conoscendo la lingua o altre proprietà della comunicazione, si possono analizzare la frequenza con cui si presentano blocchi uguali e ricavare informazioni per compiere deduzioni sul testo originale. La modalità ECB è quindi adeguata per testi molto brevi (idealmente di un blocco) o nei casi in cui la chiave cambi per ogni blocco. In compenso, un bit errato nella trasmissione del testo cifrato causa un errore di decifratura solo nel blocco interessato.

La modalità CBC (Cipher Block Chaining) utilizza il blocco di testo cifrato precedente e lo combina in XOR (OR esclusivo, un'operazione tra due bit che produce come risultato 1 se i bit sono diversi o 0 se sono uguali) con il blocco successivo di testo in chiaro prima della cifratura. Il primo blocco è combinato in XOR con un Vettore di Inizializzazione (IV, Initialization Vector), scelto con forti proprietà di pseudocasualità in modo che testi diversi producano lo stesso testo cifrato.

La decifratura funziona nel modo opposto: ogni blocco è decifrato e combinato in XOR con il blocco precedente. Il primo blocco è decifrato e combinato in XOR con il vettore d'inizializzazione.

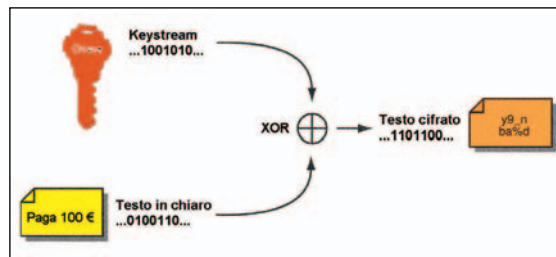
Poiché la cifratura dipende dai blocchi precedenti, un bit errato nella trasmissione del testo cifrato causa un errore di decifratura nel blocco interessato e in tutti quelli successivi. La modalità CBC assicura che le ripetizioni pre-

senti nel testo in chiaro non si riflettano in ripetizioni nel testo cifrato.

Altri modi utilizzati per i cifrari a blocchi sono il CFB (Cypher Feedback Mode), dove il blocco precedente di testo cifrato è cifrato e combinato in XOR con il blocco corrente di testo in chiaro (il primo blocco è combinato in XOR con il vettore d'inizializzazione) e l'OFB (Output Feedback Mode), che mantiene uno stato di cifratura, ripetutamente cifrato e combinato con i blocchi di testo in chiaro per produrre i blocchi cifrati (lo stato iniziale è costituito dal vettore d'inizializzazione).

Un cifrario a flusso (stream cipher) è un tipo di cifrario simmetrico che può essere progettato in modo da essere eccezionalmente veloce, molto più rapido di qualunque cifrario a blocchi. Mentre i cifrari a blocchi operano su blocchi di dati relativamente grandi (come 64 o 128 bit), i cifrari a flusso operano su unità più piccole, solitamente singoli bit. Un cifrario a blocchi produce lo stesso testo cifrato a parità di testo in chiaro, di chiave e di vettore d'inizializzazione. Con un cifrario a flusso, la trasformazione delle piccole unità di testo in chiaro varia a seconda del momento in cui esse compaiono durante il processo di cifratura.

Un cifrario a flusso genera il keystream, ossia una sequenza di bit usata come chiave, traducibile come flusso chiave, e la cifratura avviene combinando il keystream con il testo in chiaro in un'operazione di OR esclusivo (XOR), bit per bit, equivalente a una somma con eliminazione dell'eventuale riporto. La generazione del keystream può essere indipendente dal testo in chiaro e dal testo cifrato, producendo il cosiddetto cifrario sincrono, oppure può dipendere dai dati e dalla loro cifratura, nel qual caso il cifrario a flusso viene detto auto-sincronizzante. La maggior parte dei cifrari a flusso sono del tipo sincrono.



Cifrario a flusso con generazione di keystream (flusso chiave) e cifratura continua del testo in chiaro.

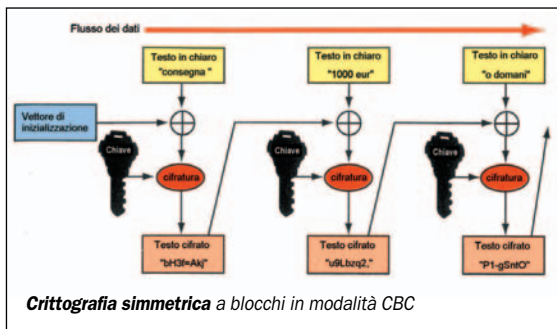
Principali algoritmi di crittografia simmetrica

Esistono diversi algoritmi di crittografia simmetrica, ognuno con le proprie caratteristiche di velocità, con specifici requisiti di risorse hardware o software e con un proprio livello di sicurezza (misurato dal tempo necessario per il "cracking", cioè la scoperta della chiave segreta). Per esempio, alcuni sono più sicuri, ma richiedono un'implementazione hardware, altri sono meno sicuri, ma presentano bassi requisiti di memoria e si prestano per l'uso con piattaforme limitate come le smartcard.

Alcuni esempi di algoritmi di crittografia simmetrica tra i più conosciuti sono: Data Encryption Standard (DES), Triple-DES (3DES), Blowfish, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Rivest Cipher #4 e #5 (RC4 e RC5) e Skipjack.

DES

Il National Institute of Standards and Technology (NIST), ex National Bureau of Standards, è una divisione del Dipartimento del Commercio statunitense, strettamente legato alla National Security Agency (NSA) che a sua volta appartiene al mondo militare. All'inizio degli anni '70, era alla ricerca di un algoritmo di crittografia da adottare come standard. Tra i produttori invitati a proporre soluzioni, IBM presentò il proprio algoritmo Lucifer a 128 bit, utilizzato per le transazioni finanziarie. Lucifer fu accettato, ma la NSA lo modificò riducendone la chiave a 64 bit (di cui 56 bit



Crittografia simmetrica a blocchi in modalità CBC

5.2.2.2 Conoscere i principali standard di crittografia simmetrica e le loro principali differenze (DES, 3DES, AES, eccetera)

Crittografia simmetrica a blocchi in modalità CBC (Cipher Block Chaining).

effettivi e 8 usati per il controllo di parità), rinominandolo Data Encryption Standard. Nel 1977 DES divenne lo standard nazionale di crittografia per le informazioni non classificate (ossia non confidenziali). Nel corso degli anni, il NIST ha ricertificato periodicamente DES attraverso i documenti FIPS (Federal Information Processing Standards Publication) 46-1, 46-2 e 46-3, fino alla fase di transizione tra DES e il suo successore AES. DES è l'algoritmo di cifratura più conosciuto ed è stato il primo di cui sono stati forniti tutti i dettagli di implementazione. È stato incluso nella maggioranza dei prodotti commerciali dotati di funzionalità crittografiche ed è stato usato dagli enti governativi. Per oltre un decennio, DES è stato considerato uno degli algoritmi più efficaci ed efficienti, finché la NSA smise di supportarlo nel 1988, prevedendo la sua vulnerabilità a fronte della crescita della potenza di calcolo dei computer. Nel 1998 DES fu violato in un attacco di tipo "forza bruta" (test di tutte le possibili chiavi) durato tre giorni, con un computer dotato di 1.536 processori. Tale fatto accelerò il processo di sostituzione di DES con 3DES (triplice applicazione di DES) e con AES. Dal 1999, DES poteva essere usato solo sui sistemi "legacy", cioè hardware o software antiquato ancora in uso, e nella pratica corrente doveva essere sostituito da 3DES e in seguito da AES.

DES è un algoritmo di crittografia simmetrica a blocchi di 64 bit secondo il modello di Horst Feistel (il crittologo di IBM che l'ha sviluppato), che prevede la divisione del blocco in due metà e una serie di sostituzioni e permutazioni in 16 passaggi con scambi tra i due semiblocchi.

3DES

Saltò il doppio DES (chiave di 112 bit) perché si dimostrò che avesse la stessa efficacia del DES, si passò alla tripla applicazione del DES (112 o 168 bit per le chiavi) prolungando il ciclo di vita di questo particolare sistema di cifratura. 3DES è 256 volte più robusto del DES, ma richiede fino al triplo di tempo per la cifratura e la decifratura. Esistono diverse varianti di 3DES:

- DES-EE3: utilizza tre diverse chiavi di cifratura
- DES-EDE3: usa tre chiavi per cifrare, decifrare e cifrare di nuovo i dati
- DES-EEE2 e DES-EDE2: come sopra, salvo che la prima e la terza operazione utilizzano la stessa chiave.

L'algoritmo alla base di 3DES è lo stesso di DES, l'algoritmo più studiato e collaudato di tutti i tempi. 3DES è molto robusto e affidabile, ma è stato progettato circa 30 anni fa ed è stato concepito per l'implementazione in hardware. A maggior ragione, 3DES è poco efficiente in software e non è considerato una soluzione valida a lunga scadenza, anche se saranno necessari parecchi anni per la sua definitiva sostituzione.

AES

Dopo che il DES era stato usato per oltre 20 anni e si avvicinava il momento del suo "cracking", il NIST decise che era tempo d'introdurre un nuovo standard di crittografia. La decisione fu annunciata nel 1977, assieme alla richiesta di candidature. Il nuovo standard avrebbe dovuto essere un algoritmo simmetrico a blocchi capace di supportare chiavi di 128, 192 e 256 bit. I finalisti furono MARS (sviluppato dagli autori di Lucifer), RC6 (di RSA Laboratories), Serpent (di Anderson, Biham e Knudsen), Twofish (di Counterpane Systems) e Rijndael (dei belgi Joan Daemen e Vincent Rijmen). Rijndael (così chiamato dai nomi degli autori) fu scelto dal NIST per sostituire il DES. È stato pubblicato dal NIST nel 2001 col nome di AES ed è l'algoritmo richiesto per proteggere le informazioni riservate, ma non classificate, del governo statunitense. AES utilizza blocchi di 128 bit, rappresentati sotto forma di matrice; ogni blocco viene cifrato in 10, 12 o 14 passaggi (a seconda della lunghezza della chiave) che comprendono operazioni di sostituzione dei byte, permutazione delle righe della

matrice, sostituzione delle colonne, combinazione XOR dei byte con una matrice (chiave espansa) ottenuta espandendo la chiave dai 128, 192 o 256 bit originari a 176, 208 o 240 byte.

L'attento scrutinio dell'algoritmo Rijndael non ha mostrato punti deboli, tanto che nel 2003 il governo USA ha autorizzato l'uso di AES per la cifratura di documenti classificati fino al livello di secret con chiave di 128 bit e di top secret con chiave di 192 o 256 bit. È la prima volta che il pubblico ha accesso ai dettagli di un algoritmo crittografico approvato per informazioni di massima segretezza. Al 2004, sono noti attacchi su 7, 8 e 9 passaggi rispettivamente con chiavi di 128, 192 e 256 bit; qualche crittografo ha espresso dubbi sulla tenuta futura del margine di sicurezza, ma, a meno di sorprese, è previsto che AES risulti sicuro per decenni a venire. AES è utilizzabile senza il pagamento di royalty.

Blowfish

Blowfish è un cifrario simmetrico a blocchi di 64 bit con chiavi di lunghezza fino a 448 bit. Durante la cifratura i dati sono sottoposti a 16 fasi di funzioni crittografiche. Blowfish è un algoritmo molto robusto ed è stato scritto da Bruce Schneier, uno degli autori più citati nel campo della crittografia.

IDEA

IDEA è un cifrario simmetrico a blocchi di 64 bit, suddiviso in 16 sotto-blocchi sottoposti a otto serie di manipolazioni matematiche. IDEA presenta similitudini con DES, ma è molto più robusto. La chiave è lunga 128 bit. IDEA è brevettato ed è concesso in licenza dalla società svizzera Mediacrypt.

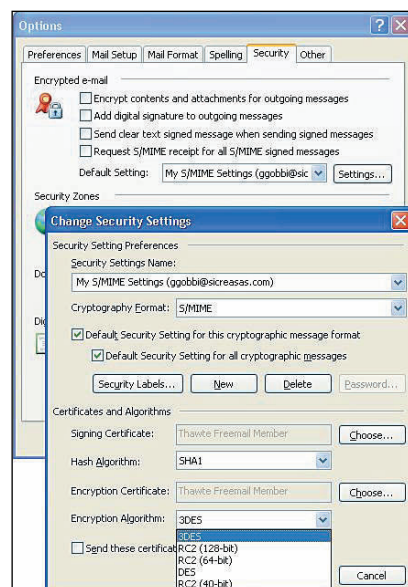
RC5

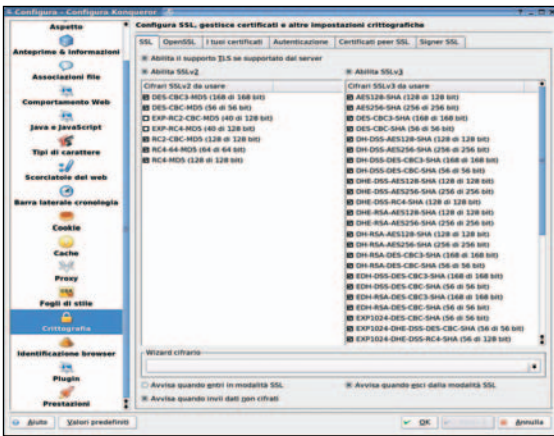
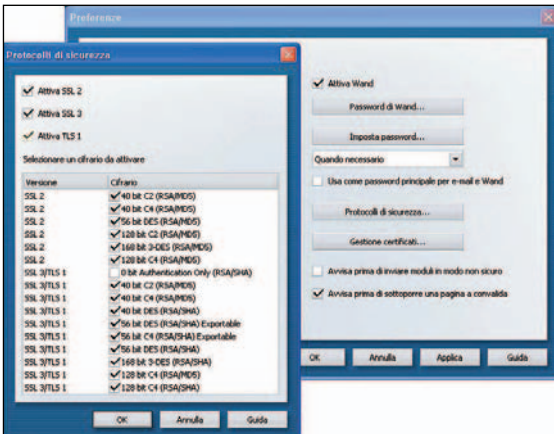
RC5 è un cifrario simmetrico a blocchi dotato di parecchi parametri per assegnare le dimensioni del blocco, la lunghezza della chiave e il numero di passaggi di trasformazione da eseguire. È stato creato da Ron Rivest (la R di RSA). Di solito si utilizzano blocchi di 32, 64 o 128 bit e la chiave può raggiungere i 2.048 bit. RC5 è stato brevettato da RSA Security nel 1997. Il basso consumo di memoria lo rendono adatto per smartcard e altri dispositivi simili.

Skipjack

Skipjack è un cifrario a blocchi sviluppato dalla NSA nel 1987, messo in servizio nel 1993 e declassificato nel 1998. Opera su blocchi di 64 bit con una chiave di 80 bit e può

Opzioni di crittografia in Microsoft Outlook





te e destinatario dei documenti segreti utilizzavano, per la cifratura e la decifratura, la stessa chiave, concordata in anticipo usando un mezzo di trasmissione non crittografico e custodita al sicuro.

Si è già accennato alle difficoltà di gestione delle chiavi simmetriche e alla proliferazione di chiavi da custodire e distribuire segretamente. Whitfield Diffie e Martin Hellmann, i primi a introdurre pubblicamente i concetti della crittografia a chiave pubblica nel 1976, si posero l'obiettivo di risolvere due dei principali problemi della crittografia simmetrica:

- 1) la necessità di condividere una chiave, precedentemente distribuita agli interlocutori, o, in alternativa, allestire un centro per la distribuzione delle chiavi (key distribution center) e
- 2) l'esigenza di associare ai messaggi e documenti cifrati una "firma digitale" equivalente a una firma autografa su carta. Diffie ed Hellmann a Stanford e Merkle a Berkeley unirono le rispettive competenze sulla crittografia a chiave pubblica e sulla distribuzione delle chiavi pubbliche rivoluzionando il mondo della ricerca crittografica, fino ad allora chiuso nelle stanze degli enti militari.

Solo in seguito, sono venute alla luce le vere e segrete origini della crittografia a chiave pubblica: a metà degli anni '60 presso la National Security Agency - NSA (secondo affermazioni del direttore dell'NSA di quel tempo, indirettamente suffragate dall'uso nell'NSA di telefoni basati su crittografia a chiave pubblica) e nel 1973 presso il britannico Government Communications Headquarters (GCHQ), i cui documenti sono stati rivelati nel 1997 dal Communications-Electronics Security Group (CESG), il braccio del GCHQ per la sicurezza delle informazioni. I documenti di Ellis e Cocks (www.cesg.gov.uk/), in assenza di documentazione dell'NSA, sono quindi i più antichi riguardo la nascita della crittografia asimmetrica. Dopo Ellis e Cocks e Diffie, Hellmann e Merkle, il terzo gruppo chiave per lo sviluppo della crittografia a chiave pubblica è stato Rivest, Shamir e Adleman, autori dell'algoritmo RSA.



La loro ricerca è quasi contemporanea ai lavori di Diffie, Hellmann e Merkle (ma basata su un diverso principio matematico) e costituisce un ulteriore passo in avanti, perché include l'implementazione della firma digitale. Oggi RSA è la sigla più spesso associata alla nozione di crittografia a chiave pubblica, ma in molte applicazioni sono utilizzate le tecnologie derivate dallo scambio chiavi di Diffie-Hellmann.

La crittografia asimmetrica, ossia a chiave pubblica, fa uso di due chiavi diverse per cifrare e decifrare i messaggi o documenti. Con un sistema di crittografia a chiave pubblica, gli utenti possono comunicare in modo sicuro attraverso un canale insicuro senza dover concordare in anticipo una chiave. Un algoritmo asimmetrico prevede che ogni utente abbia una coppia di chiavi: la chiave pubblica e la chiave privata, in relazione tra loro, ma tali che non si possa ricavare l'una dall'altra. La chiave privata dev'essere custodita al sicuro dal proprietario, mentre la chiave pubblica può essere distribuita senza restrizioni, a patto che sia autenticata. La proprietà fondamentale di un algoritmo asimmetrico è che si può cifrare un messaggio con una qualsiasi delle due chiavi, dopo di che si deve utilizzare l'altra chiave per decifrarlo.

Se Alessandro vuole spedire a Bruno un documento riservato, deve procurarsi una copia autenticata della chiave pubblica di Bruno (in pratica un certificato digitale di Bruno) e con essa cifrare il messaggio. Bruno utilizza la propria chiave privata per decifrare

Opzioni di crittografia in Opera

Opzioni di crittografia in Konqueror

Nella crittografia asimmetrica, detta anche crittografia a chiave pubblica, esiste sempre una coppia di chiavi, tra loro inseparabili: una pubblica e una privata

sfruttare le principali modalità di crittografia a blocchi: ECB, CBC, CFB e OFB. E' stato fornito in chipset preconfezionati e nella cryptocard Fortezza, una PC Card con processore di cifratura e memoria per i dati da cui costruire le chiavi. Skipjack è un cifrario molto robusto, ma la lunghezza limitata della chiave lo rende inferiore all'AES. Skipjack è utilizzato soprattutto da militari e agenzie governative USA.

RC4

RC4 è il più noto dei cifrari a flusso. E' stato creato nel 1987 da Ron Rivest per RSA Security. Utilizza un keystream di dimensioni variabili (ma solitamente di 128 bit) e opera su un byte alla volta. In origine il cifrario era segreto, ma fu fatto filtrare su Internet. L'algoritmo è molto robusto se utilizzato con chiavi di lunghezza adeguata (tipicamente 128 bit) casuali e non riutilizzate. Nel 2000 il governo USA ha rimosso la limitazione a 40 bit per l'esportazione dei prodotti con RC4. RC4 è 10 volte più veloce di DES. Due esempi di impiego sono nel protocollo SSL (Secure Sockets Layer) utilizzato dai browser Internet per lo scambio sicuro di informazioni (per esempio nelle transazioni commerciali) e nel protocollo WEP (Wired Equivalent Privacy) che è parte dello standard 802.11 per le LAN wireless.

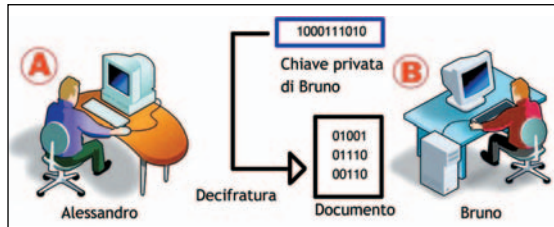
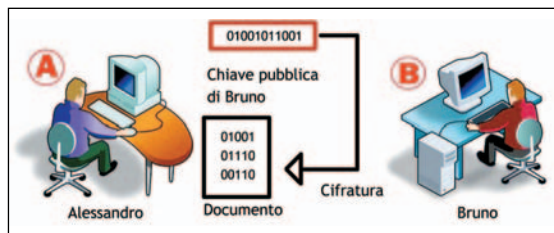
Crittografia nel PC

Le immagini seguenti mostrano alcuni degli algoritmi di crittografia supportati da Microsoft Outlook e dal browser Opera (su piattaforma Windows) e dal browser Konqueror (su piattaforma SUSE Linux).

Crittografia asimmetrica

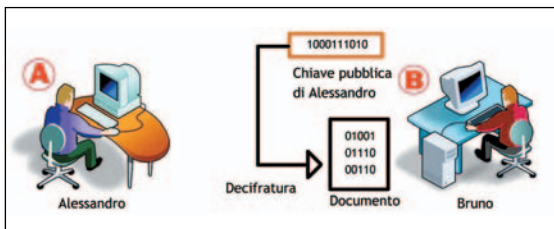
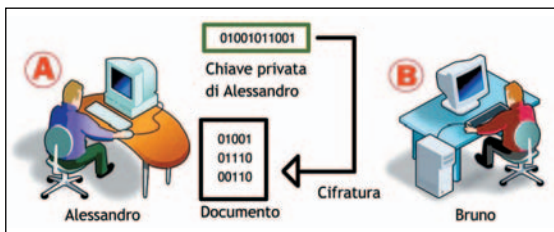
Per la maggior parte della storia della crittografia, dall'antichità nota fino a qualche decennio fa, mitten-

Impiego della chiave pubblica del destinatario per cifrare un messaggio che solo il destinatario potrà decifrare con la propria chiave segreta. Chiunque può accedere alla chiave pubblica e perciò la fonte del messaggio non è autenticabile



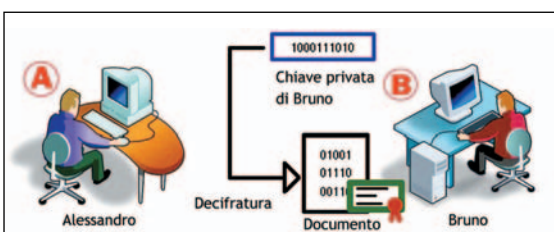
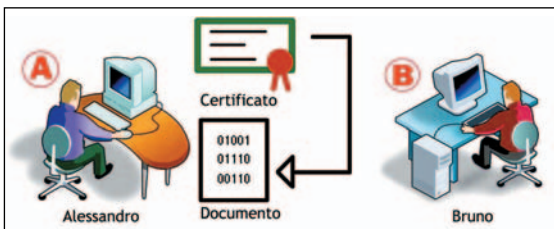
il messaggio e ricostruire il documento originale. Il messaggio rimane riservato, ma non si può essere certi della sua autenticità, ossia che sia stato spedito da Alessandro.

Se Alessandro vuole inviare a Bruno un documento



in modo da garantirne l'autenticità e l'integrità, lo cifra con la propria chiave privata, dopo di che Bruno (ma anche chiunque altro) lo decifra con la chiave pubblica di Alessandro. In questo caso manca la riservatezza.

Per assicurare riservatezza, autenticità e integrità,



Usiamo la chiave pubblica del destinatario per cifrare un messaggio che solo lui potrà decifrare con la sua chiave privata, ma aggiungiamo un certificato che autentica la nostra identità

Alessandro potrebbe utilizzare una doppia cifratura, con la propria chiave privata e con la chiave pubblica di Bruno. Questi tre scenari sono puramente didattici; in pratica, vedremo che esistono metodi più efficienti e che la crittografia asimmetrica non è usata per cifrare l'intero contenuto dei messaggi.

Torniamo al primo esempio, in cui Alessandro invia un messaggio cifrato con la chiave pubblica di Bruno. Un modo per autenticare il messaggio, dimostrando la propria identità, è quello di allegare un certificato digitale, ovvero un oggetto che associa la chiave pubblica al suo proprietario, eliminando il sospetto che il mittente sia un impostore. Un certificato digitale è rilasciato da un'autorità di certificazione (CA, Certification Authority), uno degli elementi che compongono un'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure, un sistema per la creazione e gestione delle chiavi pubbliche). Il certificato garantisce dell'identità del possessore della chiave pubblica: la coppia di chiavi viene tipicamente generata sul computer dell'utente e presso la CA viene conservata la sola chiave pubblica e il certificato che la CA ha generato sulla base di questa.

Il certificato digitale contiene varie informazioni più la chiave pubblica del suo proprietario, ed è firmato dall'autorità che lo emette per attestare la validità del certificato e del certificatore.

Un'alternativa all'uso dei certificati emessi da una CA è l'utilizzo di PGP (Pretty Good Privacy), un metodo ampiamente diffuso per cifrare messaggi e documenti tramite una coppia di chiavi che chiunque può generare, senza certificazione o con un certificato firmato, non da una Certification Authority, bensì da altri utenti fidati che formano una rete di fiducia.

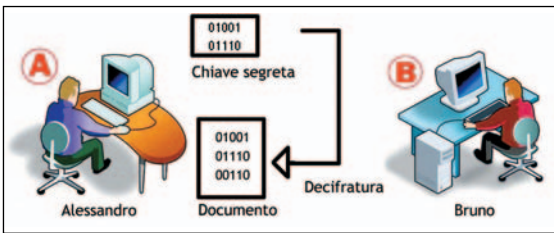
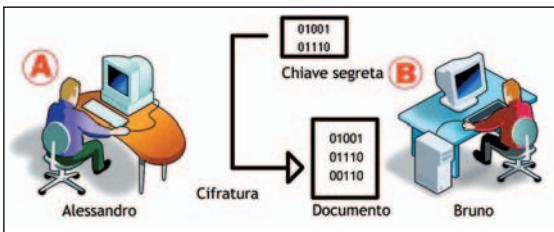
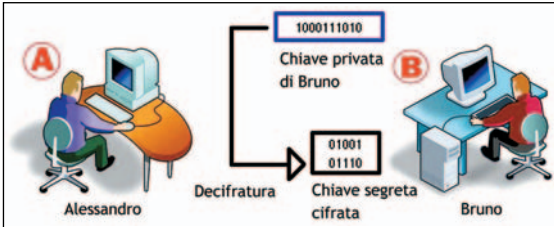
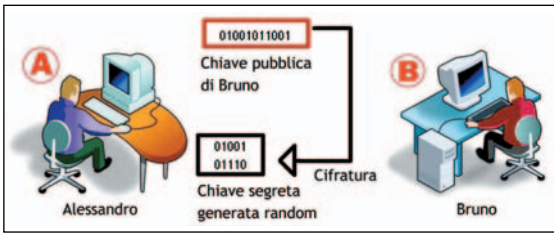
Il metodo dei certificati si basa su una struttura organizzata e comporta oneri in base alle funzionalità e modalità d'impiego.

Thawte è l'unica CA che fornisce certificati gratuiti di durata annuale per uso personale, da usare per firmare e cifrare la posta elettronica. L'uso di PGP e delle sue varianti (come vedremo in seguito) è invece più libero e informale e ha forme d'implementazione gratuite.

I cifrari asimmetrici hanno prestazioni bassissime, inferiori a quelle dei cifrari simmetrici per vari ordini di grandezza (RSA è mille volte più lento di DES). Perciò, di solito, non sono utilizzati per cifrare interi messaggi e documenti, bensì per cifrare una chiave di sessione, che a sua volta viene utilizzata per cifrare il messaggio con un cifrario simmetrico. Una chiave di sessione è una chiave temporanea "usa e getta", creata al momento e distrutta alla fine della sessione, per esempio dopo l'invio di un messaggio e-mail cifrato o alla fine di una transazione Internet con SSL (Secure Sockets Layer - il protocollo standard per transazioni sicure su Internet).

In questo scenario ibrido, che vede l'uso contemporaneo di cifrari simmetrici e asimmetrici, s'innesta un altro dei mattoni fondamentali delle applicazioni crittografiche, cioè le funzioni di hash. Una funzione di hash riceve in input un messaggio o un blocco di dati di lunghezza variabile e fornisce come risultato un valore di lunghezza fissa chiamato codice di hash (hash code o semplicemente hash) o anche message digest o hash digest.

Una tale funzione è progettata in modo che a un dato input corrisponda sempre lo stesso output e che sia minima la probabilità che input diversi generino lo stesso output (collisione). Un hash rappresenta una "impronta informatica" (fingerprint) del messaggio o documento su cui è calcolato e serve a verificare l'integrità dei dati: qualunque alterazione ai dati causa



un'alterazione dell'hash. Una funzione di hash può essere vista come una funzione di compressione o di cifratura a senso unico, perché non c'è modo di risalire dall'hash ai dati di partenza.

Standard di crittografia asimmetrica

Ci sono parecchi algoritmi di crittografia asimmetrica, ma quelli più noti, sicuri e utilizzati sono il citato RSA e quelli derivati dalla ricerca di Diffie e Hellmann, tra cui ElGamal e DSA.

RSA, dell'omonima azienda, è il cifrario asimmetrico più utilizzato. Può essere usato sia per la cifratura (per ottenere la riservatezza), sia per la firma digitale (per ottenere l'autenticazione), sia per lo scambio delle chiavi (come nell'esempio di cui sopra). Secondo RSA, una chiave asimmetrica di 1.024 bit equivale, in robustezza, a una chiave simmetrica di 80 bit (una lunghezza oggi relativamente limitata), mentre chiavi di 2.048 e 3.072 bit equivalgono a chiavi simmetriche di 112 e 128 bit. RSA raccomanda di utilizzare almeno 1.024 bit fino al 2.010, mentre 2.048 bit dovrebbero essere adeguati fino al 2.030, per poi passare a 3.072 bit. Secondo il NIST (National Institute of Standards and Technology), una chiave RSA di 15.360 bit equivale a una chiave simmetrica di 256 bit. In pratica, per chiavi importanti che si prevede di usare per molti anni, conviene passare a 2.048 bit, come già s'inizia a vedere per le chiavi di firma dei certificati digitali.

Gli algoritmi asimmetrici si basano su calcoli matematici facili da eseguire in una direzione, ma molto difficili, o pressoché impossibili da eseguire nella direzione inversa. RSA si basa sulla difficoltà di scompor-

re in fattori il prodotto di due numeri primi di grandi dimensioni. La soluzione di Diffie ed Hellmann si basa invece sul cosiddetto problema del logaritmo discreto, ovvero della difficoltà di risalire alla x nell'equazione $g^x = y \text{ mod } p$. La notazione $y \text{ mod } p$ (y modulo p) indica il resto della divisione y/p . Il metodo Diffie-Hellmann è utilizzato per lo scambio delle chiavi, dove i due interlocutori si scambiano le chiavi pubbliche e, con le proprie chiavi private, costruiscono una chiave segreta condivisa. L'algoritmo ElGamal, dal nome del suo inventore, sfrutta anch'esso il problema del logaritmo discreto, dove x è la chiave privata e p , g e y formano la chiave pubblica. ElGamal può essere usato sia per la cifratura sia per l'autenticazione con firma digitale. È un algoritmo sicuro e ha la caratteristica di generare un testo cifrato lungo il doppio del testo in chiaro.

Una variante dell'algoritmo ElGamal è il DSA, o Digital Signature Algorithm, sviluppato dalla NSA e pubblicato dal NIST (National Institute of Standards and Technology) e diventato uno standard del governo USA. DSA ha una chiave pubblica e una privata, ma viene usato solo per la firma dei documenti, non per la cifratura. DSA richiede l'uso dell'algoritmo di hash SHA (Secure Hash Algorithm), uno standard FIPS (Federal Information Processing Standard) statunitense. SHA genera un digest di 160 bit che viene passato a DSA o a un altro degli algoritmi di firma digitale ammessi dal governo USA (RSA ed ECDSA, Elliptic Curve Digital Signature Algorithm). Lo standard federale americano per la firma elettronica si chiama DSS (Digital Signature Standard), di cui DSA è l'algoritmo di firma e SHA è l'algoritmo di hash.

A parità di lunghezza di chiave, RSA e DSA hanno sicurezza comparabile.

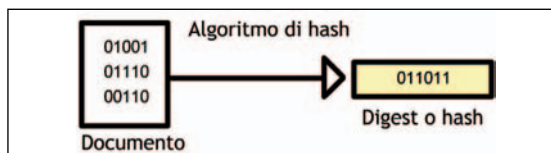
Se il problema del logaritmo discreto e la fattorizzazione del prodotto di numeri primi sono i due metodi matematici alla base dei cifrari asimmetrici più diffusi, la recente crittografia a curve ellittiche (ECC) si rivela promettente in termini di efficienza, con chiavi molto più corte. Una chiave ECC di 163 bit equivale a una chiave RSA di 1024 bit. Le curve ellittiche sono una branca della teoria dei numeri e sono definite da certe equazioni cubiche (di terzo grado); le loro proprietà permettono di creare algoritmi crittografici asimmetrici, vista l'estrema difficoltà di eseguire i calcoli a ritroso per ricostruire la chiave privata dalla chiave pubblica e dalle condizioni iniziali. Un esempio di utilizzo dell'ECC è nella ECDSA, una variante più efficiente del DSA basata sulle curve ellittiche.

Riferimenti bibliografici:

Handbook of Applied Cryptography, A. Menezes, P. van Oorschot, S. Vanstone, 1996.
Scaricabile in Pdf da www.cacr.math.uwaterloo.ca/hac
Applied Cryptography, Bruce Schneier, Second Edition, 1996
Cryptography and Network Security, William Stallings, Third Edition, 2002
Internet Cryptography, Richard Smith, 1997

Funzioni di hash e digest

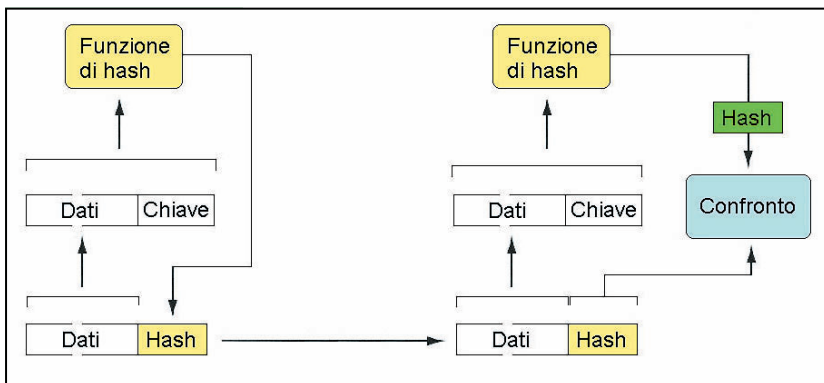
Un hash è un numero binario di lunghezza fissa, ricavato da un input (file, messaggio, blocco di dati ec-



Scambio della chiave segreta con cifratura asimmetrica RSA.

Alessandro e Bruno vogliono scambiare messaggi cifrati con crittografia simmetrica. Bruno manda ad Alessandro la sua chiave pubblica RSA ed Alessandro la usa per cifrare la chiave segreta casuale per la sessione che spedisce a Bruno in modo sicuro. Bruno decifra la chiave segreta usando la sua chiave privata RSA e quindi la usa per cifrare il messaggio. Alessandro usa la chiave segreta che ha generato per decifrare il messaggio di Bruno

5.2.3.2 Conoscere i principali standard di crittografia a chiave pubblica



Un esempio d'uso delle funzioni di hash è nel calcolo di un Message Authentication Code, che consente al destinatario di verificare la sola integrità dei dati ricevuti. I dati vengono trasmessi in chiaro in abbinamento a un MAC (MD5, SHA-1 o successivi) che è stato calcolato unendo il messaggio e la chiave segreta

cetera) di lunghezza variabile, che funge da "impronta" del dato di partenza. L'analogia con l'impronta digitale è pertinente, perché è compatta, può essere facilmente archiviata, trasmessa ed elaborata elettronicamente e consente d'identificare un individuo senza che da essa si possa risalire alle caratteristiche fisiche della persona.

In modo simile, sottoponendo un documento elettronico a un algoritmo di hash, si ottiene un dato di piccole dimensioni (tipicamente 128 o 160 bit) che identifica il documento senza permettere di risalire al suo contenuto. Il codice di hash risultante dall'applicazione di una funzione di hash a un documento, viene chiamato hash, digest o impronta informatica del documento.

Per essere efficace, un algoritmo di hash deve soddisfare i seguenti requisiti:

- può essere applicato a dati di qualunque dimensione
- produce un risultato di lunghezza fissa
- il codice di hash è relativamente facile da calcolare per qualsiasi input, rendendone pratica l'implementazione hardware e software
- per qualsiasi codice di hash h, non è praticamente possibile trovare un dato di input tale per cui l'algoritmo produca h come risultato (l'algoritmo è cioè a senso unico)
- per qualunque dato di input x, non è praticamente possibile trovare un dato y diverso da x per cui l'algoritmo produca lo stesso codice di hash (resistenza debole alle collisioni)
- è praticamente impossibile trovare una coppia di dati (x, y) tale per cui l'algoritmo produca lo stesso codice di hash quando è applicato a x e a y (resistenza forte alle collisioni)
- come corollario, la modifica di qualsiasi bit del dato di input produce una modifica del codice di hash; anche la trasposizione di due bit, che non modificherebbe una checksum (somma di controllo) per il controllo di parità, modifica il valore dell'hash.

L'espressione "non è praticamente possibile" significa che non è computazionalmente fattibile con le tecnologie correnti e con quelle prevedibili nei prossimi anni.

Un esempio di applicazione consiste nel calcolare l'hash di un messaggio e inviarlo, cifrato insieme al messaggio, in modo che il destinatario, ricalcolando l'hash dei dati con lo stesso algoritmo di hashing, possa verificare l'integrità dei dati ricevuti. Inoltre, se l'hash è stato cifrato con la chiave privata del mittente, la verifica (decifrazione dell'hash tramite chiave pubblica del mittente e confronto con l'hash ricalcolato sul messaggio ricevuto) serve anche per stabilire l'autenticità del mittente.

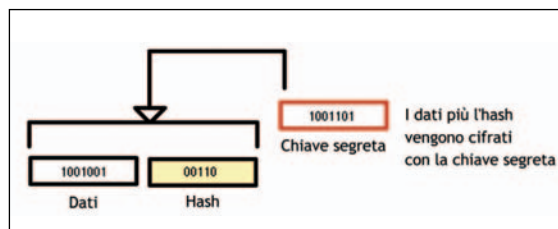
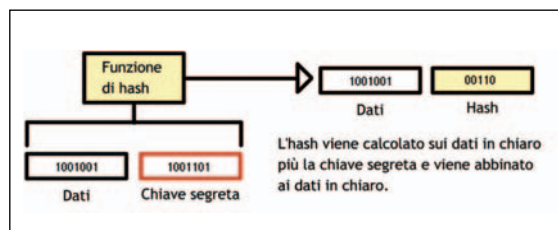
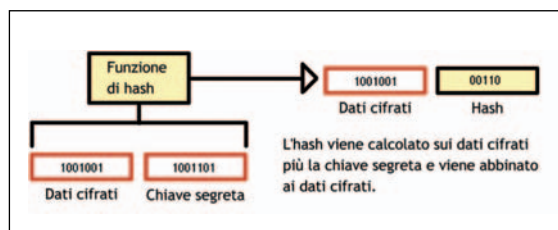
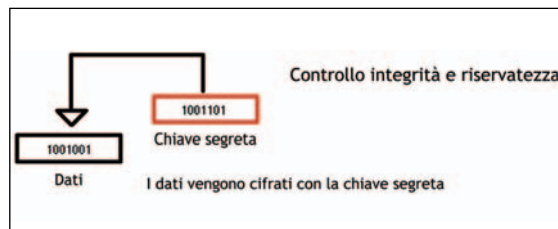
Un altro esempio di utilizzo è offerto dai Message Authentication Code (MAC), calcolati come hash del messaggio con aggiunta di una chiave segreta condivi-

sa (simmetrica).

Il messaggio viene spedito con il MAC aggiunto in coda. Il destinatario separa il MAC dai dati, aggiunge la chiave segreta e ricalcola il MAC. Se i due MAC coincidono, il destinatario sa che i dati sono integri. L'uso del MAC permette la verifica dell'integrità solo a chi è in possesso della chiave segreta. Inoltre, se qualcuno modificasse il messaggio, non potrebbe ricalcolarne il MAC senza avere la chiave segreta, quindi la modifica verrebbe scoperta.

Questa tecnica viene chiamata keyed hashing (hashing con chiave).

Il MAC assicura che il messaggio non è stato alterato e che proviene dal mittente dichiarato (nessun altro possiede la chiave segreta) si tratta quindi di un'autenticazione indiretta e non forte (visto che la chiave è nel possesso di due persone e perciò non è possibile stabilire con assoluta certezza quale delle due abbia generato il messaggio e il relativo hash). Inoltre, se il messaggio include un numero di sequenza, il destinatario ha anche la certezza che la sequenza non sia stata alterata.



Un MAC può essere usato per l'autenticazione del messaggio (come nell'esempio) o per l'autenticazione e la riservatezza (tramite cifratura). Quest'ultima può essere realizzata calcolando il MAC sul messaggio in chiaro più la chiave e poi cifrando il messaggio più il MAC generato prima usando la medesima chiave, oppure, viceversa, cifrando prima il messaggio e successivamente calcolando il MAC su messaggio già cifrato

È possibile utilizzare il MAC in abbinamento alla cifratura per garantire sia la riservatezza sia l'integrità del messaggio. L'approccio è duplice
1) si cifra il messaggio con la chiave segreta e quindi si aggiunge l'hash o digest calcolato con la stessa chiave, oppure si calcola l'hash sul messaggio in chiaro e poi si cifra messaggio più hash con la chiave segreta

più la chiave.

Il keyed hashing può essere usato anche per fornire l'autenticazione a un messaggio di tipo stream (flusso continuo), dividendo lo stream in blocchi e calcolando il MAC di ogni blocco. I MAC diventano parte dello stream e servono per verificare l'integrità dei dati ricevuti. L'uso degli hash è molto più rapido rispetto alla generazione delle firme digitali, un altro campo di applicazione delle funzioni di hash.

Un tipo speciale di MAC è chiamato HMAC ed è specificato nella RFC 2104. HMAC è anch'essa una funzione keyed hash, ma in realtà costituisce un keyed hash all'interno di un keyed hash.

Può utilizzare qualsiasi algoritmo di hash, come SHA e MD5, prendendo il nome di HMAC-SHA o HMAC-MD5. HMAC, dal punto di vista crittografico, è più robusto della sola funzione di hash di base, come è stato dimostrato da un attacco riuscito contro MD5 (una collisione creata trovando due input che producono lo stesso hash), mentre HMAC-MD5 non è stato vulnerabile a tale attacco.

Indicando con H l'algoritmo di hash utilizzato, M il messaggio e K la chiave, la funzione HMAC è definita come:

$HMAC(K, M) = H(K XOR opad, H(K XOR ipad, M))$

dove ipad è un array di 64 elementi di valore 0x36 (36 in esadecimale) e opad è un array di 64 elementi di valore 0x5C.

Tutta l'autenticazione dei messaggi in IPSEC (una famiglia di protocolli utilizzata per trasmissioni sicure su Internet) avviene tramite HMAC.

Principali algoritmi di hash

Fra i numerosi algoritmi di hash riportati in letteratura, tre sono quelli più utilizzati per le loro caratteristiche di efficienza e sicurezza: MD5, SHA-1 e RIPEMD-160.

MD5, evoluzione di MD4, è stato sviluppato da Ron Rivest all'MIT nel 1991 ed è descritto nella RFC 1321 (www.ietf.org/rfc).

MD5 è molto popolare, ma la crescita della potenza di calcolo e i primi successi degli attacchi sia basati su forza bruta sia di tipo crittoanalitico (basati sull'analisi dell'algoritmo) inducono a considerare MD5 vulnerabile e hanno suggerito lo sviluppo di nuovi algoritmi con un output più lungo dei 128 bit di MD5 e con caratteristiche specifiche per resistere agli attacchi crittoanalitici.

SHA-1 è stato sviluppato dal NIST ed è stato pubblicato come standard federale USA nel 1993 con il nome di Secure Hash Algorithm (SHA, FIPS 180) e riveduto nel 1995 come SHA-1 (FIPS180-1). SHA-1 è specificato anche nella RFC 3174 che, rispetto al FIPS 180-1, include anche un'implementazione in C.

SHA-1 riceve in input un messaggio di lunghezza massima inferiore a 264 bit (una dimensione equivalente a 2.147 Gbyte e perciò praticamente illimitata), suddiviso in blocchi di 512 bit, e produce un hash di 160 bit. Sia SHA-1 sia MD5 derivano da MD4, ma SHA-1 è notevolmente più robusto grazie ai 32 bit aggiuntivi dell'hash, che rendono molto più arduo un attacco di tipo forza bruta. Sul fronte degli attacchi crittoanalitici, MD5 ha iniziato a mostrarsi vulnerabile fin dai primi anni di vita, mentre SHA-1 non risulta vulnerabile allo stesso tipo di attacchi.

Nel frattempo sono state specificate le evoluzioni di SHA-1 a 224 bit (RFC 3874) e a 256, 384 e 512 bit di hash, talvolta chiamate ufficiosamente SHA-2 e annun-

ciate dal FIPS 180-2. I rispettivi standard si chiamano SHA-224, SHA-256, SHA-384 e SHA-512.

RIPEMD-160 è stato sviluppato nell'ambito del progetto European RACE Integrity Primitives Evaluation (RIPE) da un gruppo di ricercatori che avevano conseguito parziali successi nell'attaccare MD4 e MD5.

Inizialmente gli autori svilupparono una versione a 128 bit, ma visto che era possibile attaccare due fasi di elaborazione, decisero di espanderla a 160 bit. L'algoritmo è descritto nella norma ISO/IEC 10118-3:1998 "Information technology - Security techniques - Hash functions - Part 3: Dedicated hash-functions" (ISO, 1998).

Anche RIPEMD-160 deriva da MD4 e ha molte analogie con MD5 e SHA-1. Alla pari di SHA-1, è molto resistente ad attacchi di vario tipo; l'ulteriore complessità rispetto a SHA-1 dovrebbe rendere RIPEMD-160 ancora più protetto da attacchi crittoanalitici, benché più lento in esecuzione.

Glossario di crittografia

Algoritmo (o cifrario):

un insieme di regole logiche e matematiche usate nella cifratura e nella decifrazione.

Chiave: la sequenza segreta di bit che governa l'atto della cifratura o della decifrazione.

Crittografia:

la scienza della scrittura nascosta (o segreta) che permette di memorizzare e trasmettere dati in una forma utilizzabile solo dagli individui a cui essi sono destinati.

Crittossistema:

l'implementazione hardware o software della crittografia, che trasforma un messaggio in chiaro (plaintext) in un messaggio cifrato (ciphertext) e poi di nuovo nel messaggio in chiaro originario.

Crittoanalisi:

la pratica di ottenere il messaggio in chiaro dal messaggio cifrato senza disporre della chiave o senza scoprire il sistema di cifratura.

Crittologia:

lo studio della crittografia e della crittoanalisi.

Testo cifrato (ciphertext):

dati in forma cifrata o illeggibile.

Cifrare o cifratura:

l'azione di trasformare i dati in formato illeggibile.

Decifrare o decifrazione:

l'azione di trasformare i dati in formato leggibile.

Keyspace (spazio delle chiavi):

l'insieme di tutti i possibili valori che una chiave può assumere.

Testo in chiaro (plaintext o cleartext):

dati in forma leggibile o intelligibile.

Work factor (fattore di lavoro):

il tempo, lo sforzo e le risorse che si stimano necessarie per violare un crittossistema.

5.2.4.2 Conoscere i principali standard delle funzioni di hashing