Elementi di sicurezza informatica

Threat model

La “sicurezza” di un sistema è determinata da molteplici elementi e per ottenerla è necessario analizzare tutte le possibili minacce.

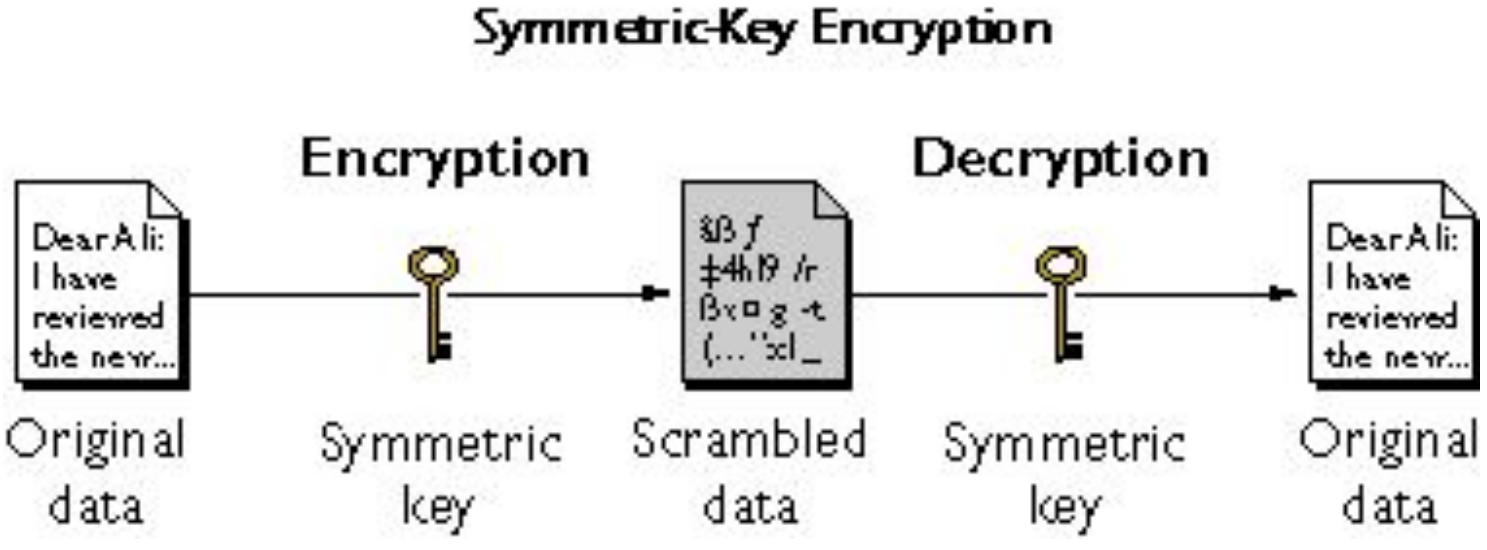
La sicurezza complessiva del sistema è determinata dal suo anello più debole.

Per ogni possibile vulnerabilità il “threat model” prende in esame le possibili minacce e le contromisure da intraprendere per poterle fronteggiare.

Principi di confusione e diffusione

- dovuti a Sahnnon (“La teoria della comunicazione nei sistemi crittografici”, 1949);
- **confusione**: la relazione tra la chiave e il testo cifrato deve essere quanto più complessa e scorrleata possibile, quindi ogni bit del testo cifrato deve dipendere da molte parti della chiave;
- **diffusione:** è la capacità dell'algoritmo di distribuire le correlazioni statistiche del testo lungo tutto l'alfabeto utilizzato dall'algoritmo di cifratura rendendo quanto più difficile possibile un attacco statistico, per cui cambiando un bit del testo in chiaro statisticamente dovrebbero cambiare la metà dei bit del testo cifrato.

Crittografia simmetrica (a chiave segreta)



Crittografia a chiave segreta

- Per ogni coppia di entità si usa la stessa chiave (segreta e condivisa) per cifrare e decifrare il messaggio;
- svantaggio: la distribuzione della chiave segreta è problematica;
- vantaggio: le prestazioni run time sono elevate;
- gli algoritmi si basano su trasposizione e sostituzione dei bit;
- esempio di implementazione: AES.

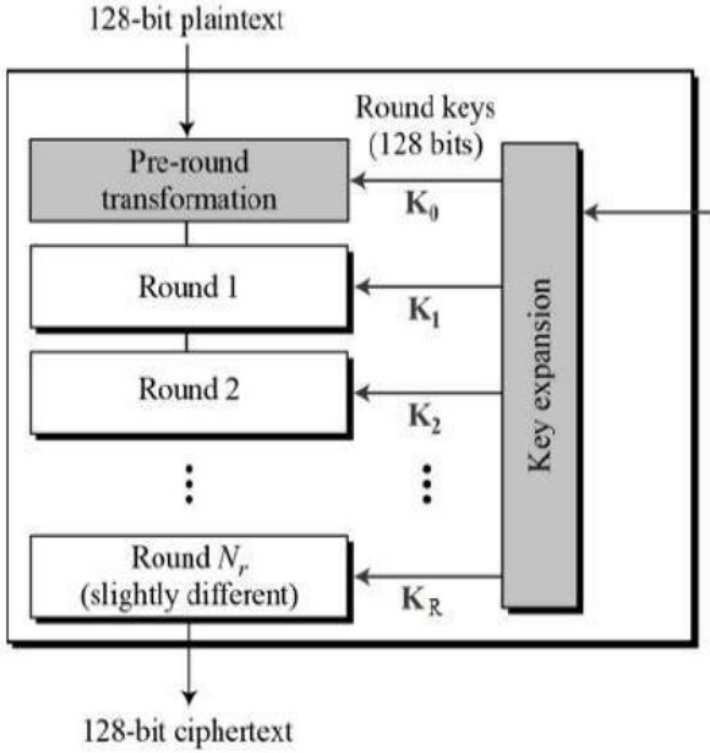
Advanced Encryption Standard

- is the cryptography algorithm adopted by US government in order to replace the older and weaker DES (Data Encryption Standard);
- is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware;
- both permutations and substitutions are applied to blocks of 16 bytes (128 bits), each block is arranged in a 4x4 bytes matrix named **state**.

Advanced Encryption Standard

The algorithm encompasses two main functions: KeyExpansion e Chiper.

KeyExpansion is a key generator that uses a procedure named Rijndael key schedule (Rijndael is the name of one of the authors of an algorithm on which AES is based), whereas Chiper is the one used in message encryption.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Advanced Encryption Standard

The size of the secret share key determines the number of rounds (repetitions of transformation) rounds that convert the plaintext into the ciphertext, more precisely:

- 10 rounds for 128-bit keys;
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on a round key generated from the secret shared key.

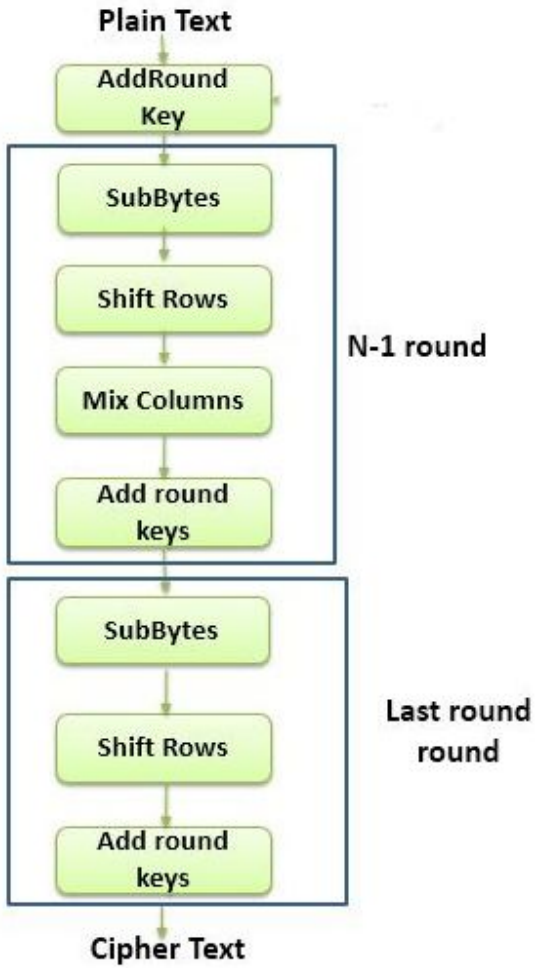
Advanced Encryption Standard

The size of the secret share key determines the number of rounds (repetitions of transformation) rounds that convert the plaintext into the ciphertext, more precisely:

- 10 rounds for 128-bit keys;
- 12 rounds for 192-bit keys.
- 14 rounds for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on a round key generated from the secret shared key.

Advanced Encryption Standard

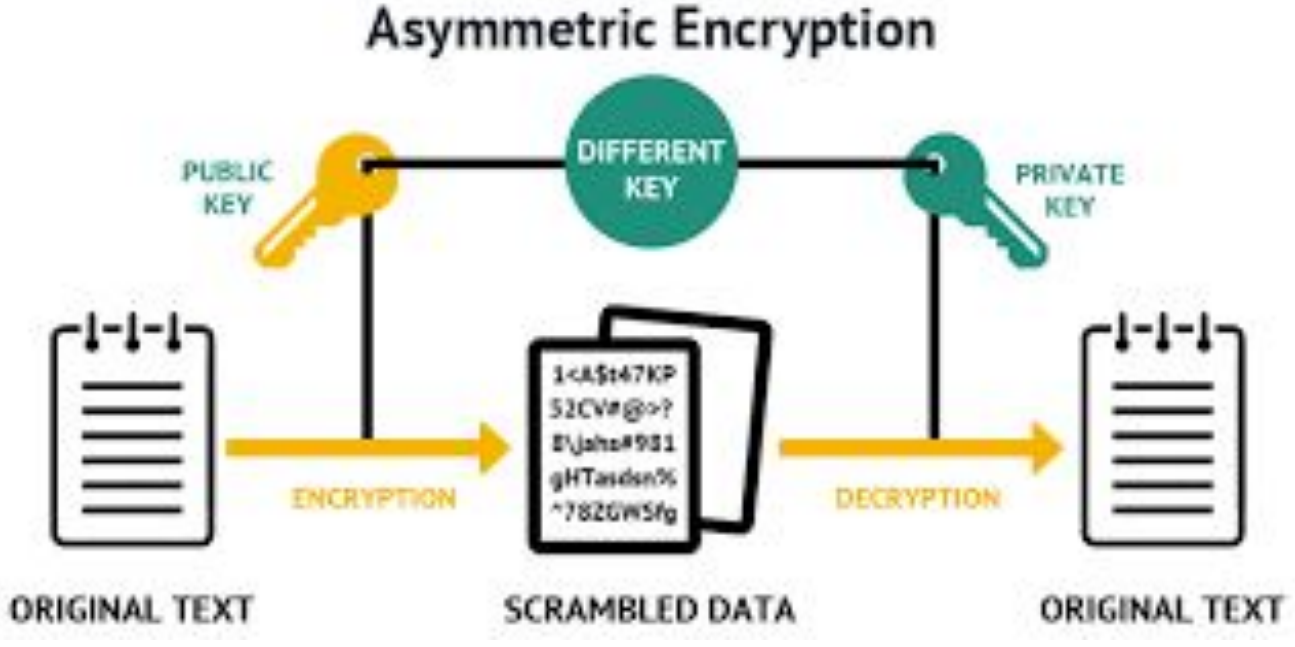


Advanced Encryption Standard

- SubBytes (byte substitution): the 16 input bytes are substituted by looking up a fixed table S−box (substitution box) given in AES design. The result is in a matrix of four rows and four columns.
- Shiftrows: each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows:
  - First row is not shifted.
  - Second row is shifted one byte position to the left.
  - Third row is shifted two positions to the left.
  - Fourth row is shifted three positions to the left.

  The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.
- MixColumns: Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.
- Addroundkey: The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Crittografia asimmetrica (a chiave pubblica)



Crittografia a chiave pubblica

- Ogni entità possiede due chiavi, una privata ed una pubblica. Per ottenere la confidenzialità, i messaggi vengono cifrati con la chiave pubblica del destinatario e decifrati con la sua chiave segreta;
- vantaggio: la distribuzione della chiave pubblica è semplice, anche se può essere necessario verificare l'associazione chiave pubblica-entità corrispondente (certificati, web of trust);
- svantaggio: le prestazioni run time sono basse;
- gli algoritmi si basano su proprietà dell'aritmetica modulare;
- esempio di implementazione: RSA.

RSA

- inventato nel 1977 da Ronald Rivest, Adi Shamir e Leonard Adleman;
- si scelgono a caso due numeri primi, **p** e **q** molto grandi;
- si calcola il loro prodotto **n=pq** e il prodotto **φ(n)=(p-1)(q-1);**
- si sceglie poi un numero **e** (esponente pubblico), primo rispetto a φ(n) e più piccolo di φ(n);
- si calcola il numero **d** (esponente privato) tale che **ed=1 mod φ(n)**

La chiave pubblica è **(n,e)**, mentre la chiave privata è **(n,d)**.

La robustezza dall'algoritmo è legata all'impossibilità computazionale di fattorizzare n.

RSA

Si divide il testo in blocchi di k bit con 2^k<=n

Ogni blocco rappresenta un numero P<n

Per cifrare

C=(P^e)modulo n (k bit)

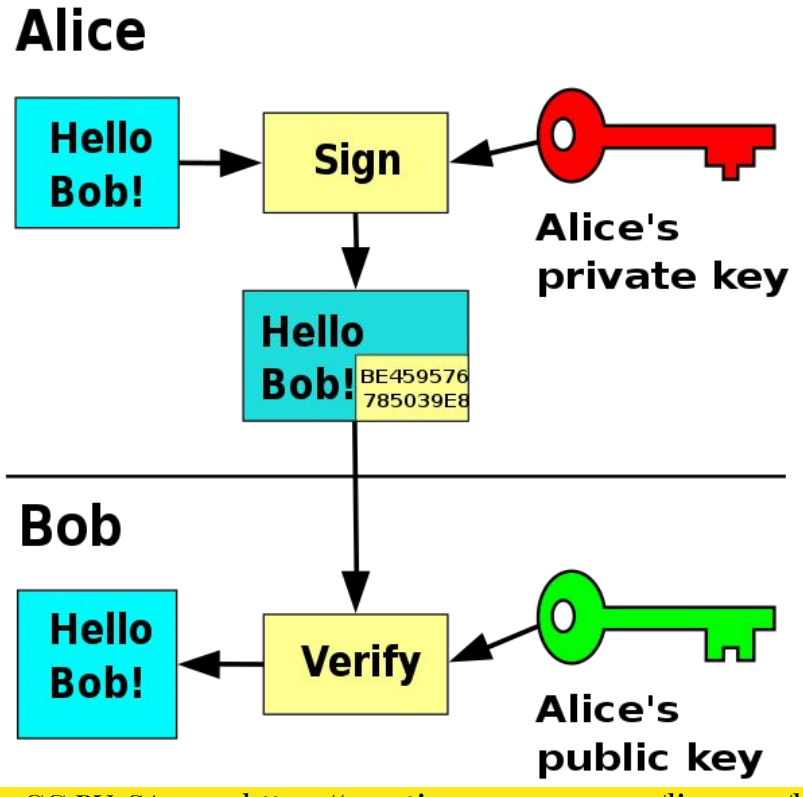
Per decifrare

P=(C^d) modulo n (k bit)

Chiave segreta di sessione

- combina i vantaggi della crittografia asimmetrica e simmetrica;
- usando la crittografia asimmetrica si realizza un canale “sicuro” tramite il quale si determina una chiave segreta, su cui successivamente si basa la comunicazione;
- nel definire la chiave segreta si utilizzano degli elementi (nonce, timestamp, contatori) per garantire la freschezza e impedire attacchi di replica.

Firma digitale



Funzioni hash

Una funzione hash è una funzione (a ogni elemento del dominio associa uno e un solo elemento del codominio) non invertibile che mappa una stringa di lunghezza arbitraria in una di lunghezza predefinita.

Per le funzioni hash utilizzate nei protocolli crittografici deve essere computazionalmente impossibile trovare una stringa con un determinato hash.

Inoltre è importante che messaggi simili producano hash diversi.

Firma digitale

- il mittente calcola un hash (es. SHA-2) del messaggio e lo cifra con la propria chiave privata ottenendo così la firma;
- la firma viene inviata assieme al messaggio;
- per verificare la firma, il ricevente calcola sul messaggio ricevuto lo stesso hash e decifra la firma con la chiave pubblica del mittente;
- se i due risultati coincidono il messaggio è **integro** e **autentico**.

Firma digitale

?

Come essere sicuri dell’identità associata a una chiave pubblica?

Certificati digitali

“Nella crittografia asimmetrica un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.”

(da Wikipedia, l’enciclopedia libera, voce “certificato digitale”)

Certificate authority

“In crittografia, una Certificate Authority, o Certification Authority (CA; in italiano: "Autorità Certificativa"[1]), è un soggetto terzo di fiducia (trusted third part), pubblico o privato, abilitato ad emettere un certificato digitale tramite una procedura di certificazione che segue standard internazionali e in conformità alla normativa europea e nazionale in materia.”

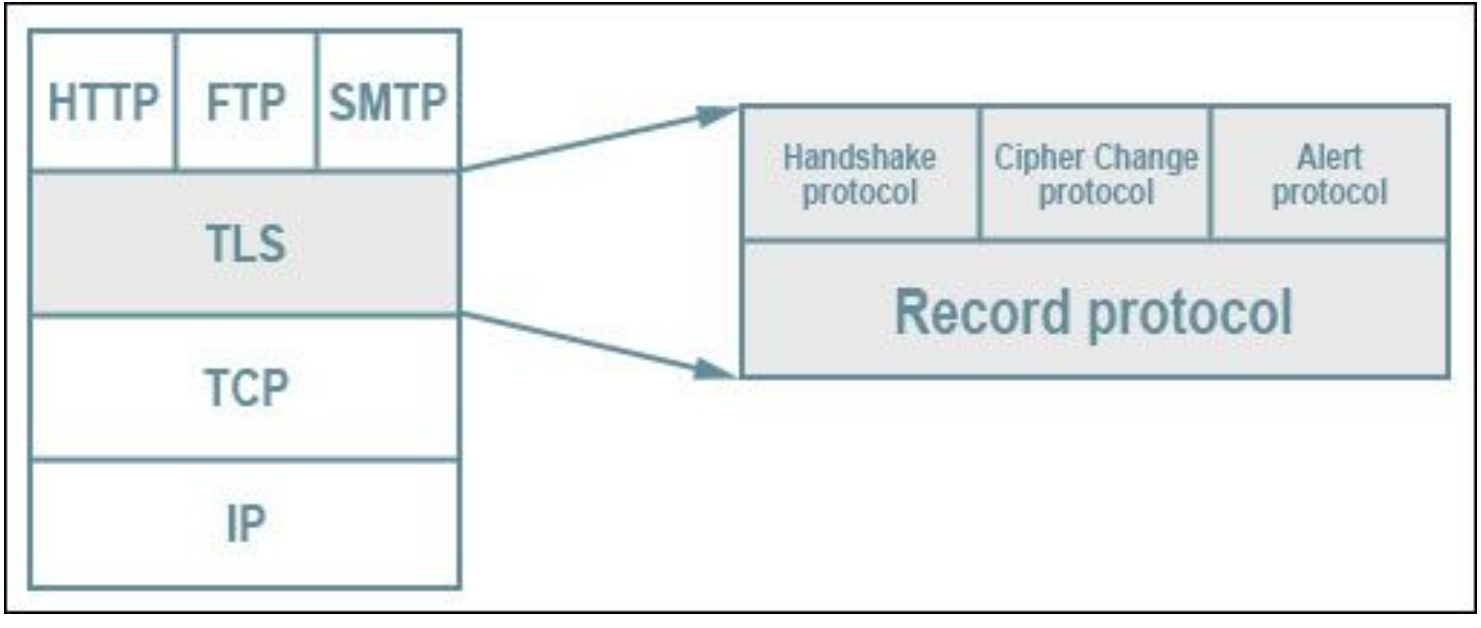
(da Wikipedia, l’enciclopedia libera, voce “certificate authority”)

Web of trust

È un sistema di certificazione, alternativo alle CA, utilizzato da PGP, GnuPG, OpenPGP e simili.

Si parte dalla conoscenza “diretta” di una persona e della sua chiave pubblica, si “firma” un certificato per questa persona, si accettano tutti i certificati firmati da membri del web of trust.

TLS: Transport Layer Security

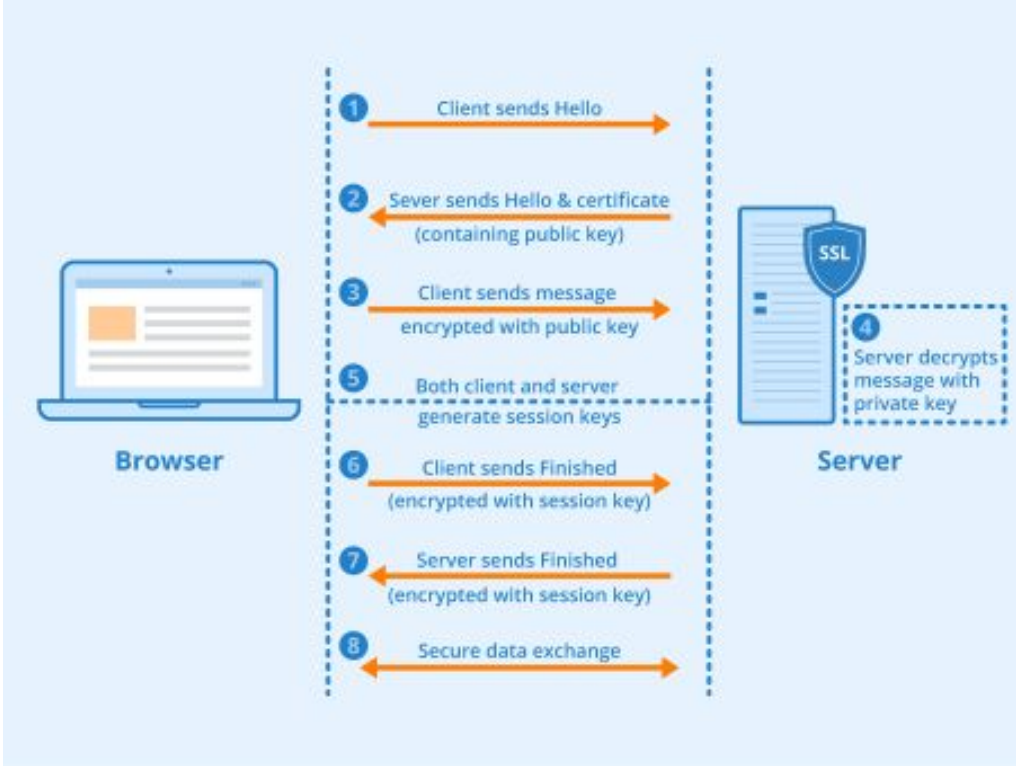


Web security: protocollo HTTPS

- Http+TLS

- Obbiettivi:
  - autenticazione del server;
  - confidenzialità;
  - autenticità/integrità;
  - freschezza

HTTPS

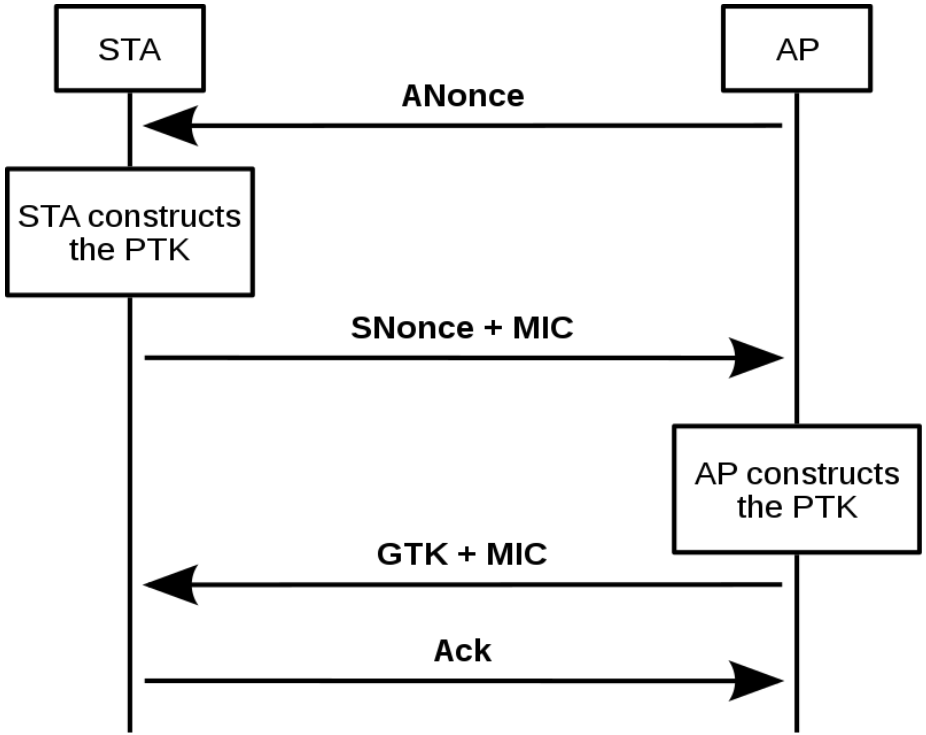


Https: handshake protocol

Per determinare la chiave segreta di sessione:

- il client e il server si scambiano i loro nonce e stabiliscono quale versione di TLS (o SSL) usare;
- il server invia una catena di certificati, in modo che il client possa verificare l'identità del server;
- il client invia una pre-master key cifrata utilizzando la chiave pubblica del server (solo il server sarà in grado di decifrare il messaggio);
- utilizzando i due nonce e la pre-master key, entrambe le parti sono in grado di calcolare la chiave segreta di sessione;
- si passa alla comunicazione cifrata utilizzando la chiave segreta di sessione.

WPA2 home edition



WPA2 handshake

L'access point AP invia un valore Anonce al client STA; il client ha tutti i dati per generare la chiave, che dipende da Anonce, Snonce, indirizzi MAC di entrambi e password della rete.

STA invia (in chiaro) il valore Snonce ad AP con in più il MIC (Message Integrity Code) cifrato.

Ora anche AP ha gli elementi per calcolare la chiave e verificare il MIC.

AP invia un messaggio cifrato contenente la group key (da usare per le comunicazioni broadcast) e un numero sequenziale insieme a un codice di integrità.

Infine STA invia la conferma ad AP.

WPA2 Enterprise

Si basa sull'utilizzo di certificati.

La stazione si collega con l'AP e invia il proprio certificato.

L'AP verifica la validità del certificato collegandosi a un server radius e successivamente viene definita una chiave segreta per la comunicazione tra il client e l'AP.

VANTAGGI:

- non è possibile per altre stazioni della rete "indovinare" la chiave;
- l'amministratore di rete può facilmente rimuovere il certificato;
- il traffico può essere univocamente associato al certificato.