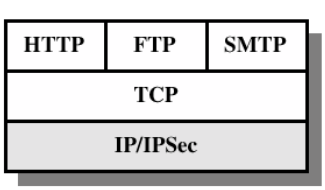
Sicurezza delle email, del livello di trasporto e delle wireless LAN

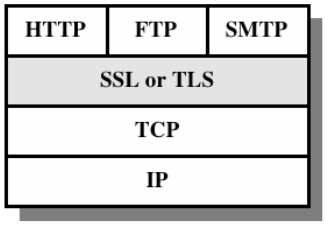
Damiano Carra

Università degli Studi di Verona
Dipartimento di Informatica

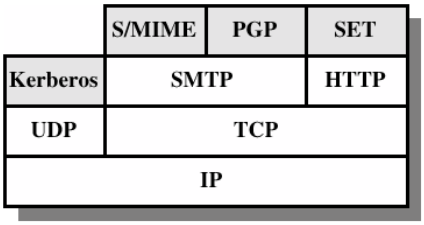
La sicurezza nello stack protocollare TCP/IP



Livello di rete



Livello di trasporto



Livello di applicazione

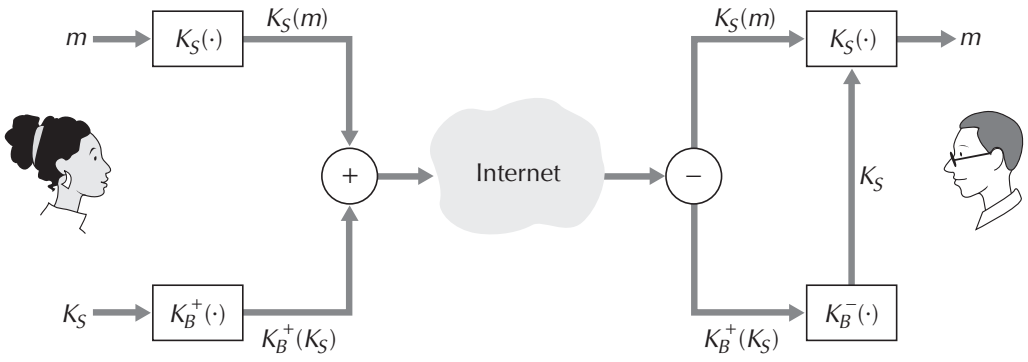
Parte I: Sicurezza delle email

Rendere sicura la posta elettronica

- Caratteristiche di sicurezza:
  - riservatezza
  - autenticazione del mittente
  - integrità
  - autenticazione del ricevente
- Per ottenere riservatezza
  - cifrare il messaggio con una chiave simmetrica (DES o AES);
  - crittografia a chiave pubblica (tramite RSA)

Esempio di schema (1)

- Alice utilizza la chiave simmetrica, KS, per inviare una e-mail segreta a Bob

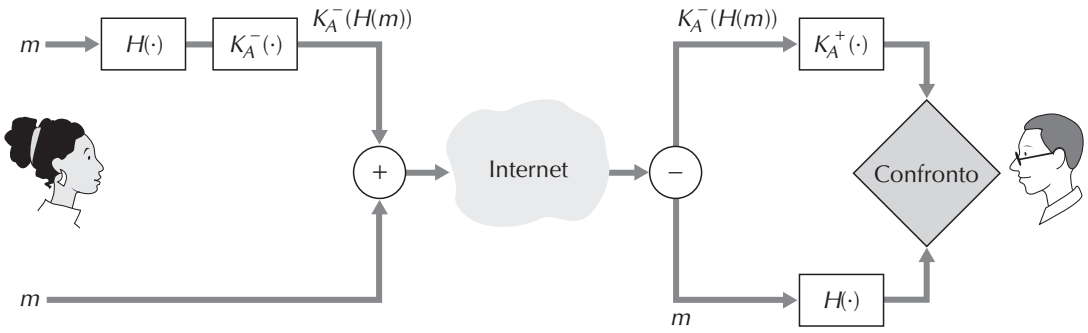


Alice invia l'e-mail *m*

Bob riceve l'e-mail *m*

Esempio di schema (2)

- Utilizzo di funzioni hash e di firme digitali per l'autenticazione e l'integrità del messaggio

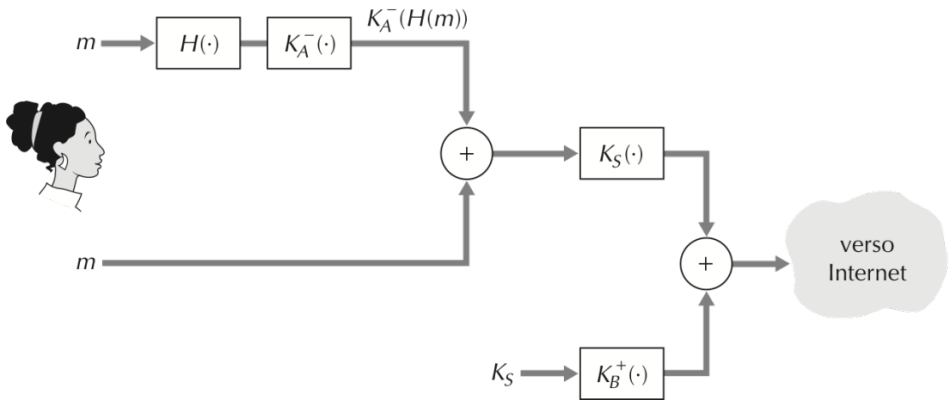


Alice invia l'e-mail *m*

Bob riceve l'e-mail *m*

Esempio di schema (3)

- Alice utilizza la crittografia a chiave simmetrica, quella a chiave pubblica, una funzione hash e la firma digitale per ottenere segretezza, autenticazione del mittente e integrità del messaggio



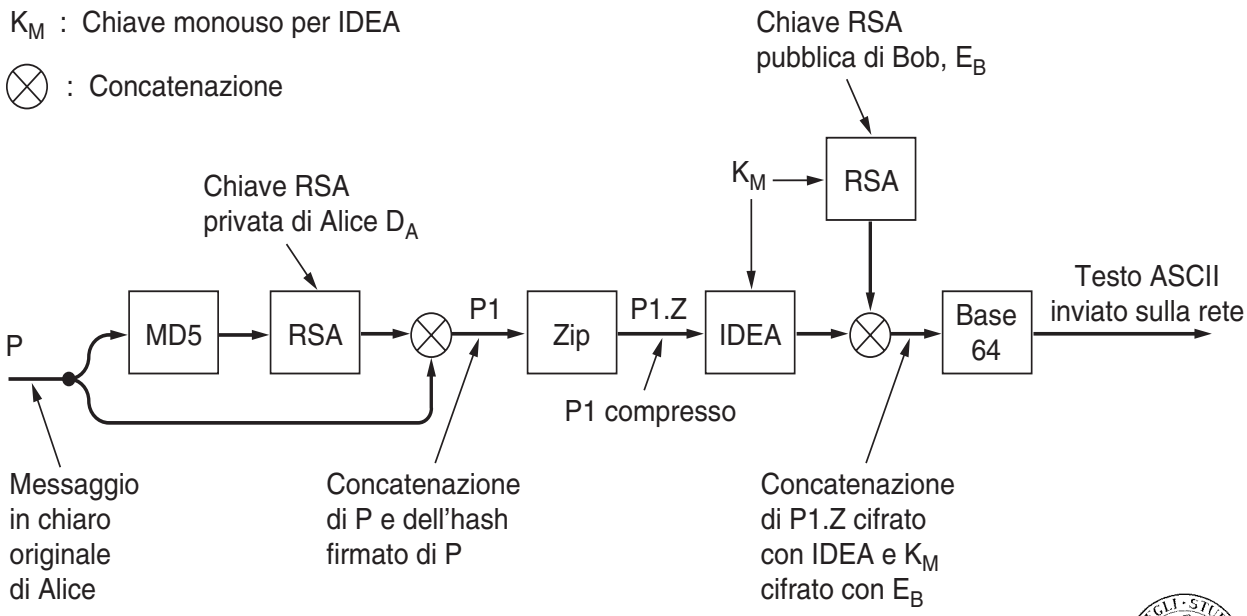
PGP (Pretty Good Privacy)

- Programma per lo scambio sicuro di messaggi testuali (confidenzialità, autenticazione)
- Sviluppato da P. Zimmerman, simbolo del diritto alla privacy elettronica
- Integra algoritmi di crittografia consolidati
- E' indipendente dall'architettura e dal sistema operativo
- Sorgenti, librerie e documentazione disponibili gratuitamente su Internet

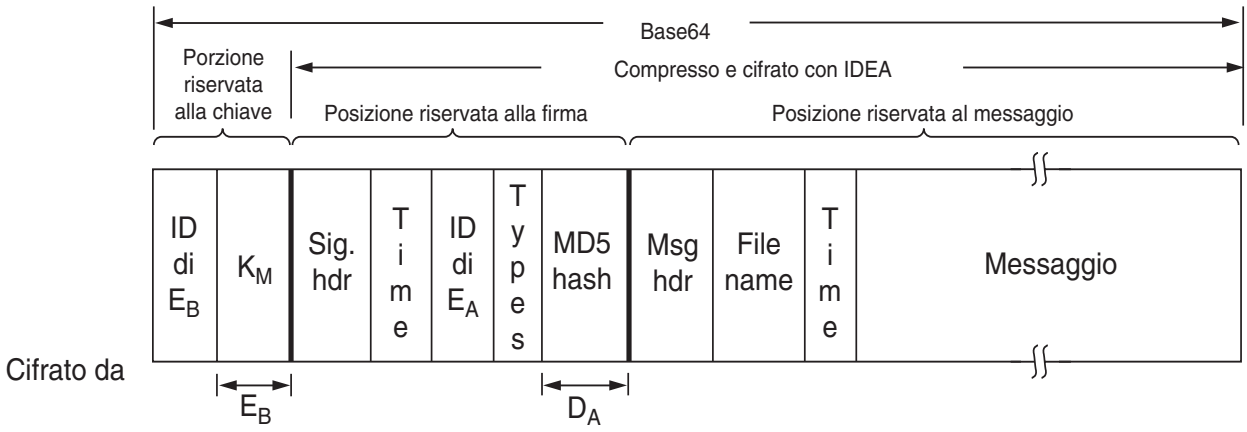
PGP: servizi offerti

- Autenticazione
  - SHA-1, RSA
  - supporta firme staccate
- Confidenzialità
  - CAST-128 o IDEA o Triplo DES
  - si utilizza una chiave di sessione one-time
- Compressione
- Codifica per compatibilità
  - radix-64
- Segmentazione

Invio di un messaggio con PGP



PGP: formato dei messaggi



Esempio di messaggio PGP firmato

```
———-BEGIN PGP SIGNED MESSAGE———-
Hash: SHA1
Bob:
Possiamo vederci stasera?
Appassionatamente tua, Alice
———- BEGIN PGP SIGNATURE ———-
Version: PGP for Personal Privacy 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
———-END PGP SIGNATURE———-
```

Esempio di messaggio PGP segreto

```
— — -BEGIN PGP MESSAGE— — -
Version: PGP for Personal Privacy 5.0
u2R4d+/jKmn8Bc5+hgDsqAewsDfrGdszX68liKm5F6Gc4sDfcXyt
RfdS10juHgbcfDssWe7/K=lKhnMikLo0+1/BvcX4t==Ujk9PbcD4
Thdf2awQfgHbnmKlok8iy6gThlp
— — -END PGP MESSAGE— — -
```

PGP: uso della fiducia

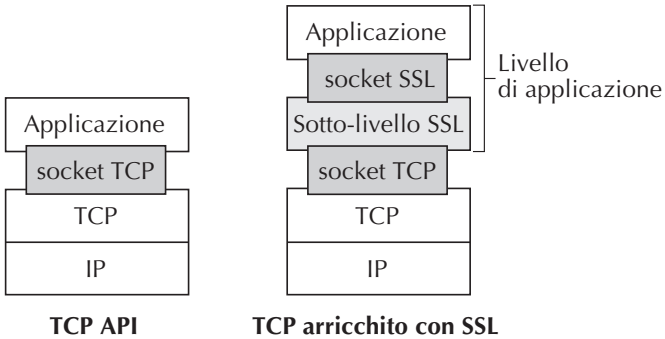
- È compito dell'utente assegnare un livello di fiducia ad ogni conoscente ed intermediario
  - il campo owner trust esprime il grado di fiducia nel proprietario come certificatore; è assegnato dall'utente (unknown, untrusted, marginally trusted, completely trusted)
  - il campo signature trust esprime il grado di fiducia nel firmatario come certificatore; è uguale a owner trust se il firmatario è tra i conoscenti, altrimenti vale unknown
- il PGP assegna il livello di fiducia nell'abbinamento chiave pubblica - utente
  - il campo key legitimacy viene calcolato dal PGP in base al valore dei campi signature trust

14

Parte II: Sicurezza del livello di trasporto

Rendere sicure le connessioni TCP: SSL

- Secure sockets layer (SSL)
  - Versione di TCP arricchita con servizi di sicurezza, comprese riservatezza, integrità dei dati e autenticazione del client e del server
  - Ci si accorge che viene usato SSL dal browser quando l'URL inizia con https anziché http



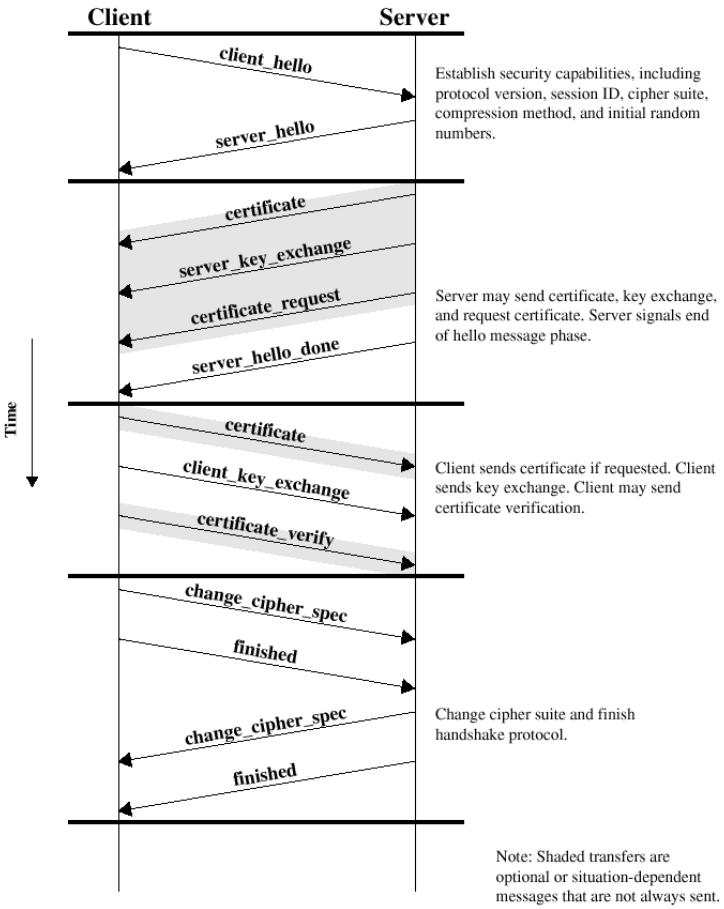
SSL/TLS

- Protocollo progettato inizialmente da NETSCAPE con il nome di SSL, specificatamente per la protezione delle transazioni web
- Divenuto standard IETF, a partire dalla versione 3.0, (RFC 2246) con il nome TLS
- Principalmente focalizzato sulle proprietà di Confidenzialità e Integrità del traffico di rete

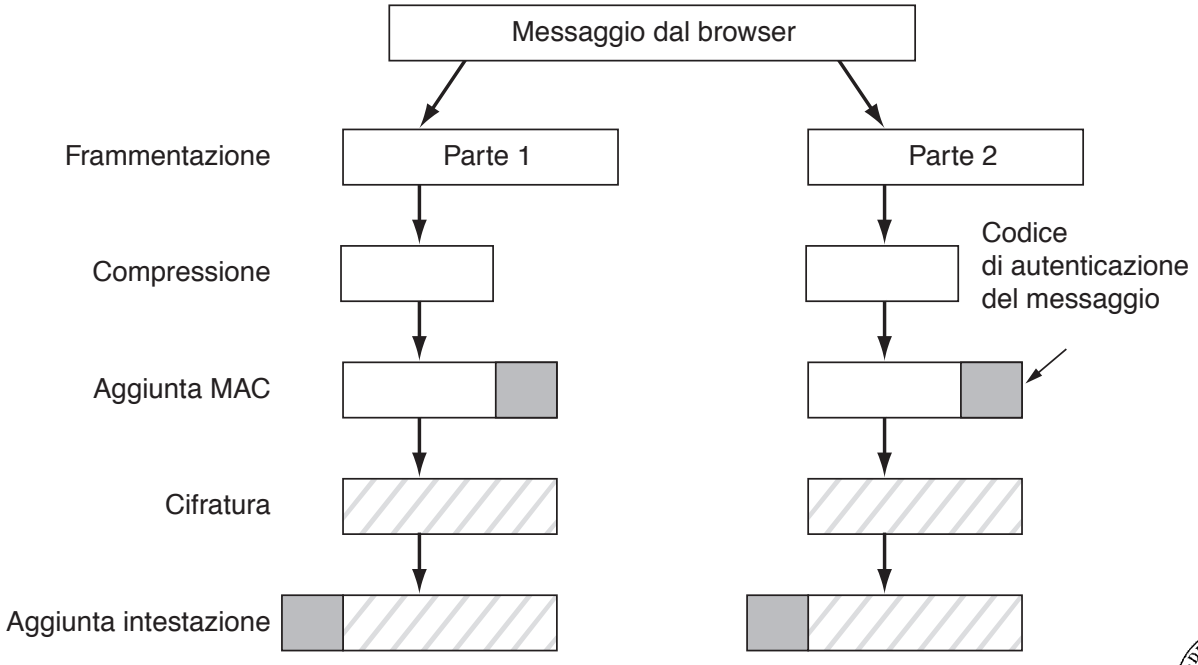
SSL/TLS: Handshake

- la fase di handshake provvede a:
  - Opzionalmente: autenticare le parti
    - Autenticazione del solo server
    - Mutua autenticazione
  - Accordare le due parti sugli algoritmi crittografici da usare
  - Generare le chiavi di sessione per la cifratura dei dati

Handshake



Trasmissione dei dati con SSL



Parte III: Sicurezza delle wireless LAN

Wired equivalent privacy (WEP)

- Protocollo 802.11 progettato per dare sicurezza ai dati in transito su reti wireless (…ma poco sicuro!!!)
  - Pensato per assicurare un livello di sicurezza simile a quello delle reti cablate

- Fornisce autenticazione e codifica dei dati tra terminale e access point wireless con un approccio a chiave simmetrica condivisa.

WEP: Autenticazione e Crittografia

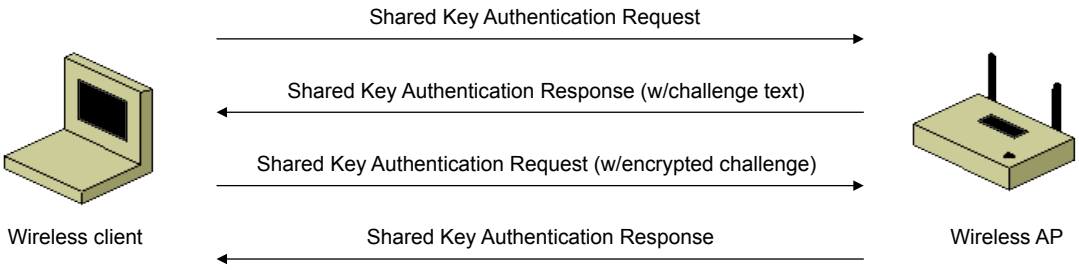
- Lavora al livello data link
- Richiede la stessa secret key condivisa tra tutti i sistemi in comunicazione (host e AP)
- Fornisce Autenticazione e Crittografia
  - Autenticazione generata utilizzando cifratura Challenge/Response
  - Autenticazione per device e non per utente

WEP: Metodi di autenticazione

- Shared key:
  - L'AP invia un testo di challenge in chiaro ad ogni device che cerca di comunicare
  - Il device che richiede l'autenticazione cripta il testo di challenge e lo invia all'AP
  - Se il testo di challenge è criptato correttamente l'AP ritiene autenticato il device
  - C'è un problema fondamentale: Testo in chiaro e testo criptato sono entrambi disponibili agli attaccanti

802.11 shared key authentication

- Scambio di 4 messaggi che usano una chiave segreta condivisa
- E' possibile effettuare attacchi di "brute force" per individuare la chiave segreta condivisa



Vulnerabilità di WEP

- Buone intenzioni
  - Usa una secret key
  - Checksum cifrato (con shared key) per garantire l'integrità dei dati
  - Usa l'algoritmo di cifratura RC4
- Però
  - La chiave è "condivisa"
  - Initialization Vector (IV) usato per cifratura è di soli 24 bit (RC4 consente IV di 40 - 128 bit)
- Protocollo vulnerabile ("eavesdropping" & "tampering")
- Possibili compromissione di confidentiality e data integrity
- Scarso controllo di accesso

802.11i

- Emendamento creato appositamente per la sicurezza
- Concetto critico di Robust Security Network (RSN)
- Una WLAN è considerata RSN se tutti i dispostivivi usano la Robust Security Network Authentication (RSNA)

- Wi-Fi Protected Access (WPA)
  - WPA e WPA2 forniscono le seguenti caratteristiche crittografiche:
    - Crittazione dei dati, usati con gli standard di autenticazione 802.1X
    - Integrità dei dati
    - Protezione da attacchi di tipo “replay”
    - Operano a livello MAC (Media Access Control)

WPA: Caratteristiche di sicurezza

- Contiene un sottoinsieme delle feature di sicurezza che sono nello standard 802.11i
- Autenticazione con EAP
- Cifratura e data integrity
  - Temporal Key Integrity Protocol (TKIP) rimpiazza WEP per alcune operazioni
  - Nuovo algoritmo di message integrity check (MIC)
  - WPA definisce l’uso di Advanced Encryption Standard (AES) come un sostituto opzionale per la cifratura WEP (dipende dalle funzionalità hardware)
- WPA risolve molte delle debolezze di WEP

WPA2: Caratteristiche di sicurezza

- Rispetta lo standard IEEE 802.11i
- WPA2 Enterprise
  - Usa 802.1X and EAP per l'autenticazione
- WPA2 Personal (WPA2-PSK)
  - Usa una preshared key per l'autenticazione
- Encryption methods
  - TKIP
  - AES

WPA2

- Attualmente è il più sicuro
- Richiede un aggiornamento del firmware
- Nelle autenticazioni 802.1x usa una cache che gli permette di utilizzare il FAST ROAMING (PMK cache, Pairwise Master Key)
- AES è obbligatorio (vengono cifrati 128 bit di dati alla volta con una chiave di cifratura a 128 bit!)