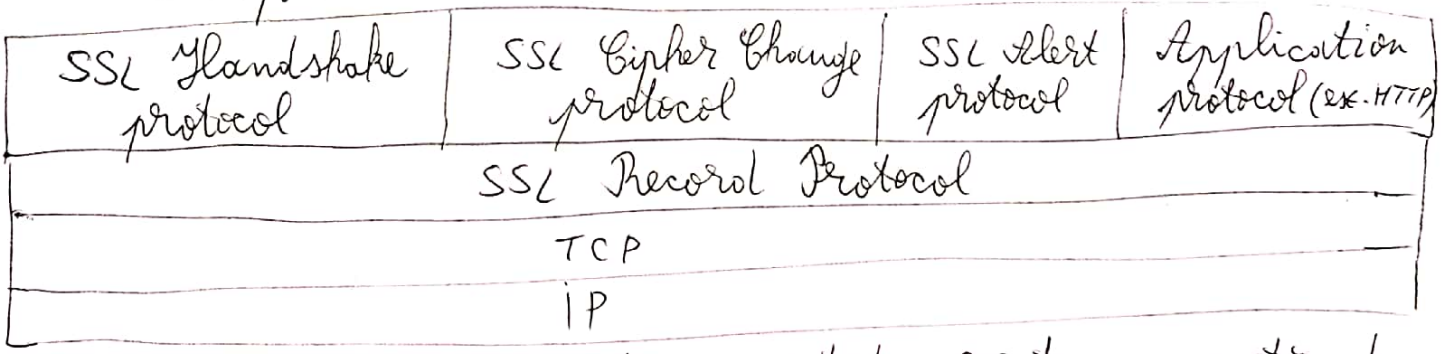
C13

SSL (Secure Socket Layer)

- protocol de securitate care asigură comunicare sigură în internet. TLS (Transport Layer Security), succesorul lui, împreună cu SSL, permit aplicațiilor client/server să comunice în așa fel încât să fie evitată "capturarea, modificarea sau falsificarea mesajelor".
  Application Layer: HTTP, LDAP și POP3
  Network Layer: SSL și TCP/IP.
- scop: securitate pt. tranzacțiile în internet.
- se împarte în 2 niveluri:
  - nivelul cel mai de jos → SSL Record → securitate date
  - protocoale de conexiune: SSL Handshake, SSL Change Cipher, SSL Alert Protocol.
- execută:
  - fragmentarea și comprimarea datelor.
  - integritatea mesajului (se creează un MAC).
  - confidențialitatea și încapsularea datelor
  - crearea unui obiect nou numit înregistrare
  - criptarea noului obiect și transmiterea lui prin TCP



- stabilește parametrii de securitate printr-o suită de cifruri și secrete criptografice. Combinația dintre schimbul de chei, metodele hash și alg. de criptare definește o suită de cifruri care se stabilește pt. fiecare sesiune SSL. Fiecare suită începe cu SSL ca termen, apoi alg. de schimb de chei și „WITH" ca separator.
  Ex.: SSL_DBE_RSA_WITH_DES_CBC_SHA.

C13

Protocolul Handshake.

- constă în:
  - clientul trimite un mesaj „client hello" la care serverul răspunde cu „server hello", altfel apare o eroare fatală și conexiunea eșuează.
  - val. din aceste 2 mesaje sunt fol. pt. stabilirea caracteristicilor de securitate între client și server.
  - se generează și se interschimbă cele 2 mesaje.

Sesiuni și conexiuni

SSL
- o sesiune între 2 sisteme este o asociere ce poate dura un timp lung.
- o conexiune poate fi stabilită și întreruptă de mai multe ori de-a lungul unei sesiuni.

Protocolul Alert (SSL)

- transmite mesaje de avertizare în timpul sesiunii.
- conține „warning" sau „fatal".
  ↓
  termină sesiunea SSL.

Protocoale de securitate legate de poșta electronică

- Serverul de e-mail dispune de 2 protocoale diferite corespunzătoare a 2 interfețe: cea pt. clienți și cea pt. ansamblul sistemului poștal. Comunicarea cu clienții se face prin protocolul POP3 (Post Office Protocol 3) care asigură distribuirea mesajelor.
- Interfața cu alte servere de e-mail se face prin protocolul SMTP (Simple Mail Transfer Protocol), prin care serverul recepționează/expediază corespondența clienților în/din Rețeaua Globală. D.p.d.v. al securității, mesajele pot fi interceptate de către persoane neautorizate. Se folosește criptarea pt. asigurarea confidențialității și autenticității mesajelor.

Protocol PGP (Pretty Good Privacy).

- asigură un serviciu utilizat pt. e-mail și aplicații de stocare de fișiere.
- utilizează cei mai buni algoritmi criptografici existenți care sunt integrați într-o aplicație de uz general lansată pe un set restrâns de comenzi ușor de folosit.
- are 5 servicii:
  - autentificare (schemă de semnătură digitală).
  - confidențialitate (criptare mesaje).
  - compresie (stocarea fișierului).
  - compatibilitate cu e-mail (folosește conversia radix-64)
  - segmentare (și reasamblare).
- pt. a asigura confidențialitatea:
  1. expeditorul generează un mesaj și un nr. aleator de 128 biți folosit ca și cheie de sesiune.
  2. mesajul este criptat cu IDEA/TDES
  3. Cheia de sesiune este criptată cu RSA utilizând cheia publică a destinatarului și adăugată mesajului.
  4. Destinatarul folosește RSA cu cheia sa privată pt. a decripta cheia de sesiune.
  5. Se decriptează mesajul.
- semnătura este generată înainte de compresie deoarece pt. stocare este preferabil să se memoreze textul clar împreună cu semnătura. Criptarea mesajului se aplică după compresie pt. a mări securitatea criptografică.
- algoritmul de compresie este ZIP.
- radix-64 expandează mesajul cu 33%, raportul de compresie fiind în medie 2. La recepție, blocul primit este convertit în radix-64 în binar.
- formatul unui mesaj PGP are 3 componente:
  - mesaj (conține datele de transmis/stocat).
  - semnătură (opțional)
  - cheie de sesiune (opțional)

C13

Protocolul PEM (Privacy Enhanced Mail)

- scop: asigurarea securității transmisiilor între utilizatori
- servicii oferite:
  - confidențialitatea mesajelor.
  - autentificarea originii mesajelor.
  - integritatea legăturii în rețea.
  - nerepudierea mesajelor prin dovedirea originii
- serviciile sunt divizate în:
  - toate mesajele prelucrate în PEM incorporează facilitățile de autentificare, integritate și nerepudiere
  - confidențialitatea este un serviciu opțional.