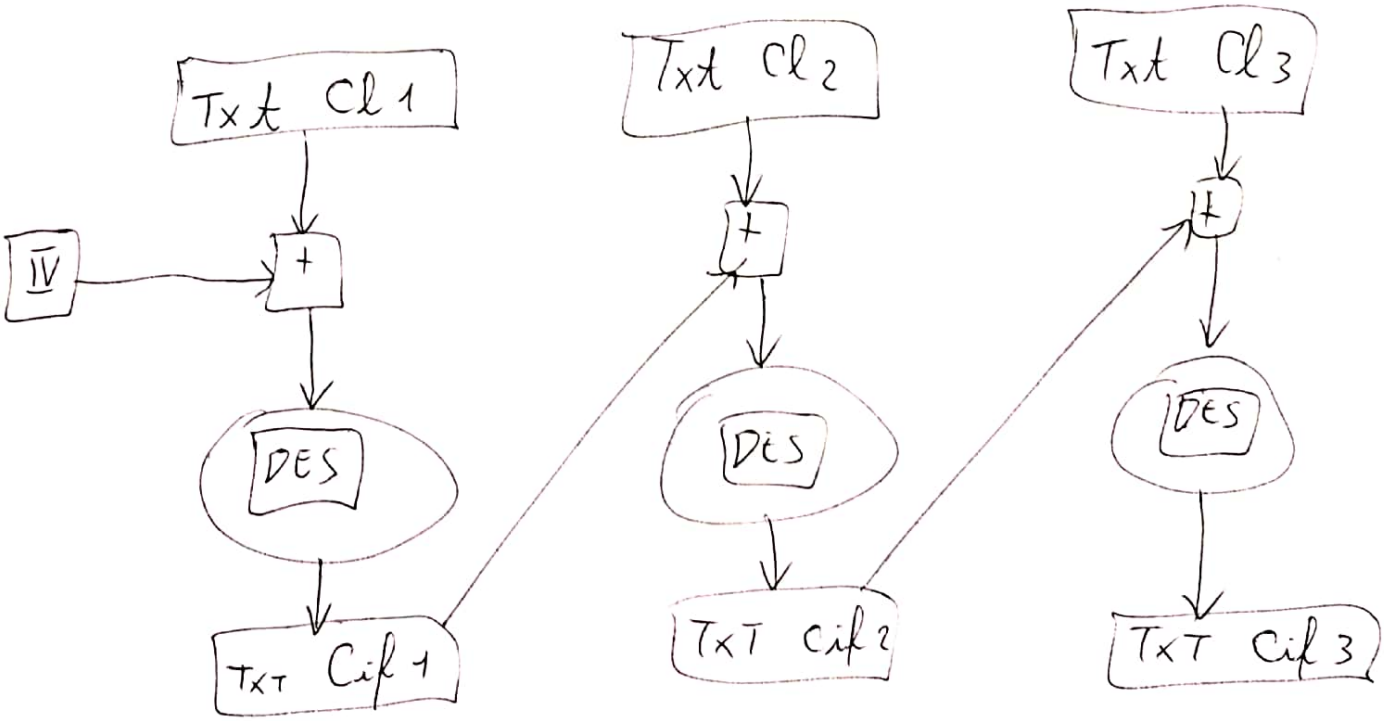
C11

Înlănțuirea blocurilor de cifrare (CBC - Cypher Block Chaining)

Lungime de [64 biți → DES / >64 biți → CBC] pt. blocuri de date criptate

CBC: se efectuează XOR între textul cifrat pt. blocul i cu textul clar al blocului i+1. Pt. blocul rezultat se execută DES. Pt. blocul 0 se folosește un vector de inițializare (IV)



C11

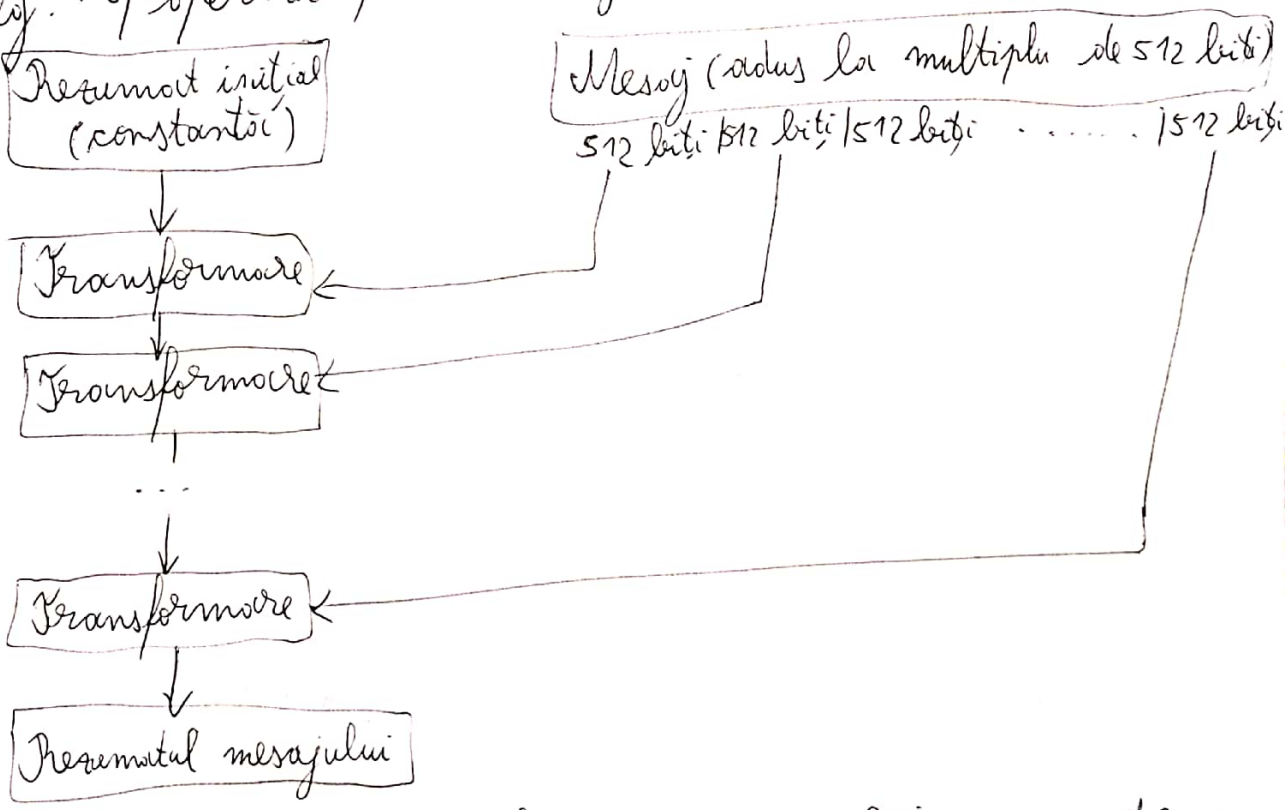
Sisteme bazate pe trunchierea mesajului

MD = Message Digest.

D. p. d. v. matematic, alg. de trunchiere a MD calculează o sumă de control de lungime constantă dintr-un mesaj de intrare de lungime arbitrară.

Algoritmii MDn și SHA (Secure Hash Algorithm) se bazează pe complexitatea alg. ce produce o ieșire aleatoare a. î. să fie îndeplinite urm. cerințe: pt. o ieșire dată, găsirea unui mesaj care să producă exact aceeași ieșire este o pb. extrem de dificilă d. p. d. v. computațional.

Alg. ~~co~~operează pe un mesaj de 512 biți.



Nucleul alg. MD5 este transformarea care preia ca intrare valoarea curentă a rezumatului (de dimensiune 128 biți) plus 512 biți ai mesaj și determină un nou rezumat (de asemenea de 128 biți). MD5 operează cu cantități de 32 biți. Rezumatul curent poate fi reprezentat ca 4 cuvinte de 32 biți (d_0, d_1, d_2, d_3), iar porțiunea curentă a mesaj ca 16 cuvinte de câte 32 de biți ($m_0 - m_{15}$).

Principalele transformări efectuate de MD5 pot fi împărțite în 4 pași.

→ Pași:
1. Se produce o nouă valoare a rezumatului pe baza valorii vechi și a mesajului de 16 cuvinte folosind 16 pași.
Ex.: $d_0 = (d_0 + F(d_1, d_2, d_3) + m_0 + T_1) \leftarrow 7$
$d_1 = (d_3 + F(d_0, d_1, d_2) + m_1 + T_2) \leftarrow 12$
....
"$\leftarrow n$" produce permutare circulară la stânga cu n biți
$F(a, b, c)$ este o combinație de operații pe biți (NOT, AND, OR) aplicate argumentelor, T_i fiind constante.
2. Diferențele față de pasul 1 sunt:
- F este înlocuit cu G, iar $T_1 - T_{16}$ cu $T_{17} - T_{32}$.
- Nr. de rotiri la stânga este $\{5, 9, 14, 20, 5, 9, \ldots\}$ la fiecare pas.
- În loc de a lua cuvintele mesajului în ordinea $m_0 - m_{15}$, la pasul i luăm cuvântul $m_{((5i+1)\%16)}$.
3. Diferențele față de pasul 1 sunt:
- F este înlocuit cu H (care este XOR)
- Folosim $T_{33} - T_{48}$ și rotirile $\{4, 11, 16, 23, 4, 11, \ldots\}$
- Cuvântul folosit la pasul i este $m((3i+5)\%16)$
4. Diferențele față de pasul 1 sunt:
- F este înlocuit cu I (care este o combinație de operații pe biți OR, XOR și NOT pe argumente.
- Folosim $T_{49} - T_{64}$ și rotirile $\{6, 10, 16, 21, 6, 10, \ldots\}$.
- Cuvântul folosit la pasul i este $m((7i)\%16)$

→ DES și MD5 sunt cu câteva ordine de mărimi mai rapizi decât RSA atunci când sunt implementați software. RSA este folosit pt. a cripta cantități mici de date (cheie/nr secret).

C11

Protocoale de integritate a mesajului

→ O modalitate de a asigura integritatea mesajului este de a-l cripta cu DES, folosind CBC și apoi să folosească restul CBC (ultimul bloc de ieșire al procesului CBC) ca fiind codul de integritate al mesajului (MIC - Message Integrity Code).

Semnătura digitală

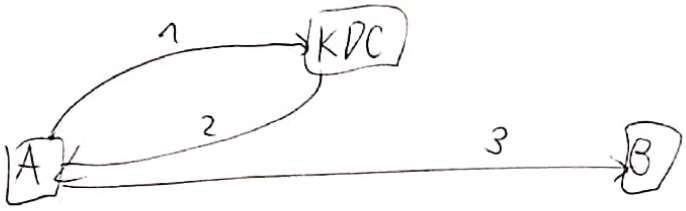
→ Este un caz special al codului de integritate al mesajului în care codul a fost generat numai de către un participant.
→ Este o modalitate de a codifica un mesaj electronic, a.î. destinatarul mesajului poate distinge cine a trimis acel mesaj.
→ Folosind RSA, un participant oarecare va folosi cheia lui privată pt. a produce semnătura lui digitală cu RSA. Folosind propria lui cheie, orice alt participant poate verifica această semnătură.

Distribuirea manuală a cheilor

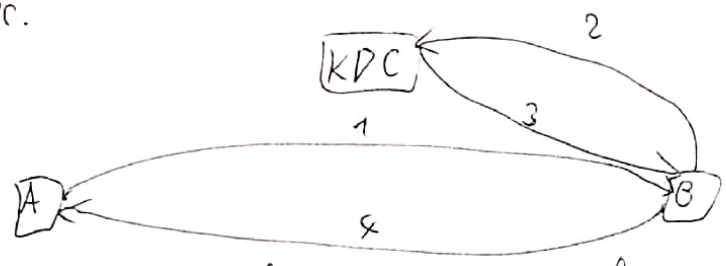
→ Folosește metode de distribuție offline pt. a distribui cheile între perechi sau la mai mulți participanți.
→ Dezavantaje: este dificilă, are pb. de securitate și nu oferă o autentificare decât cea oferită în mod implicit.
→ Distribuirea manuală a cheilor este necesară doar o singură dată pt. un utilizator anume - cheie de cifrare a cheilor (KEK - Key Encryption Key).
→ Avantaj: este mai eficientă pt. distribuția cheilor de grupuri mari.

Distribuirea bazată pe centru

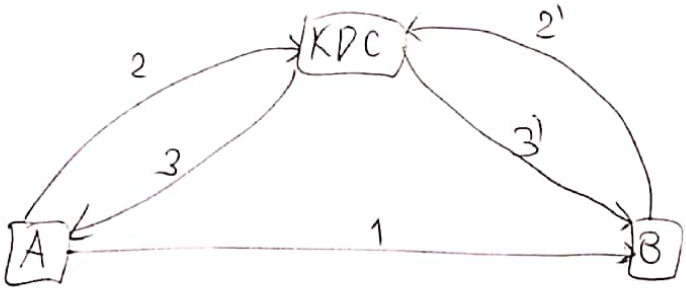
→ Se folosesc pt. a distribui chei între 2+ părți prin intermediul unui tert, credibil, precum:
1. Un centru de distribuție a cheilor (KDC)] depind de KEK.
2. Un centru de translație a cheilor (KTC)]
→ Când A necesită o cheie pt. a comunica cu B, Kerberos cere ca A să obțină o cheie de la KDC înainte.



→ În contrast, standardul american ANSI (X9.17) cere ca A să contacteze mai întâi pe B, apoi B să obțină cheia de la KDC.



→ În rețele locale, clienții obțin cheile (distribuirea efortul, care altfel ar fi preluat de câteva servere)
→ În rețele mari, este opusul (costul conectivității între clienți și KDC necesită Kerberos).
→ Modelul mixt:



Certificarea cheilor

→ Un certificat de cheie publică reprezintă o structură de date folosită pt. a se putea asocia în mod sigur o cheie publică la niște atribute (informații de identificare/autorizare) de utilizator.

C11

→ În structura certificatului sunt următoarele câmpuri:
- versiunea
- nr. serial
- alg. de semnătură
- emitent
- subiect
- valabilitate
- cheie publică subiect
- semnătura

→ Revocarea certificării este posibilă și necesară atunci când un CA este spart.