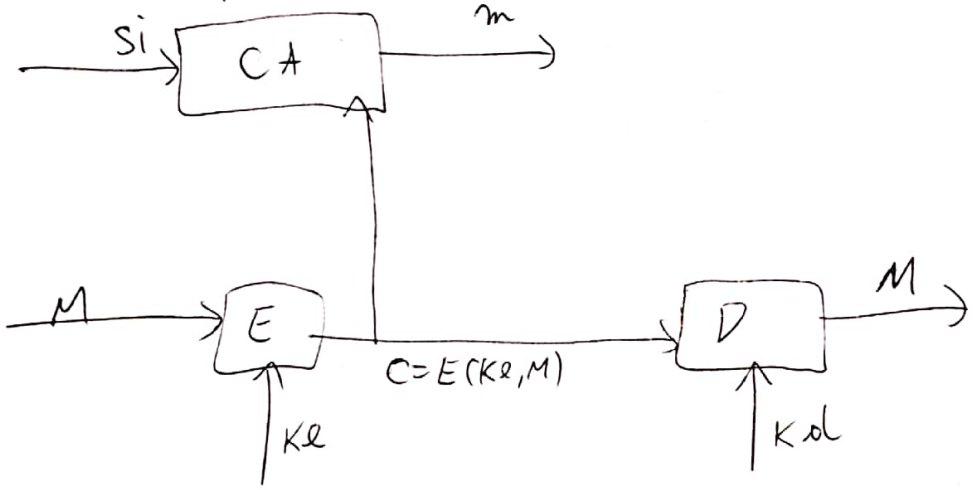
C10

Criptarea și descriptarea datelor

→ Criptarea este procesul care realizează transformarea textului clar în text cifrat pe baza unor algoritmi. Atât criptarea, cât și decriptarea necesită un parametru numit cheie. Textul cifrat (C) este transmis pe un canal nesigur către o destinație, unde este criptat.

Text clar = M
Cheie = Kc
C = E(Kc, M), E = blocul care execută criptarea.
D = operația de decriptare



Kd = cheie decriptare
M = D(Kd, C)
CA = bloc care desemnează un intrus care vrea să descifreze mesajul.

→ Exemple de informații laterale:
- frecvența literelor și cuvintelor.
- contextul canalului.
- anumite părți ale lui M

→ Atac la textul cifrat = o amenințare la un sistem în care un intrus poate avea acces numai la textul cifrat.

→ La baza proiectării sistemelor de criptare stau principiile lui Shannon:
1. Principiile de difuzare (necorelarea dintre cheie și subșirurile de caractere ale textului clar).
2. Principiile dezordonării (ieșirea să nu fie într-o relație evidentă cu intrarea).

→ Tipuri de sisteme moderne ← cu chei private (Shannon)
bazate pe chei publice.

- Criptori:
→ Cifrul lui Caesar (nr. cheilor = 25) → laborator 10.
→ Substituirea simplă (permutare de litere). Nr. permutări = 26!
→ Cifrul cu Transpoziție → laborator 10

- Criptografia modernă:
→ criptografia cu cheie secretă / permutarea biților unui cuvânt
\ substituția înlocuiește o intrare pe m biți cu o ieșire pe n biți

Fazele substituției:
1. Intrarea din m biți este convertită în forma zecimală.
2. Ieșirea zecimală este permutată
3. Rezultatul este transformat într-o formă binară pe n biți

→ Algoritmul standard de criptare a datelor (DES)
- datele sunt criptate pe blocuri de 64 biți, cu o cheie pe 56 biți.

→ Pentru fiecare mesaj M, D(E(M)) = M
Cunoașterea lui E nu compromite securitate (nu se poate deduce D din E)

- Metoda RSA (Rivest-Shamir-Adleman)
→ un text binar este împărțit în blocuri de n biți.
→ cheia de criptare publică este perechea $(e, n) \in Z$.
→ $\boxed{C = M^e \% n}$
→ $\boxed{M = C^{cd} \% n}$, avem perechea (d, n).

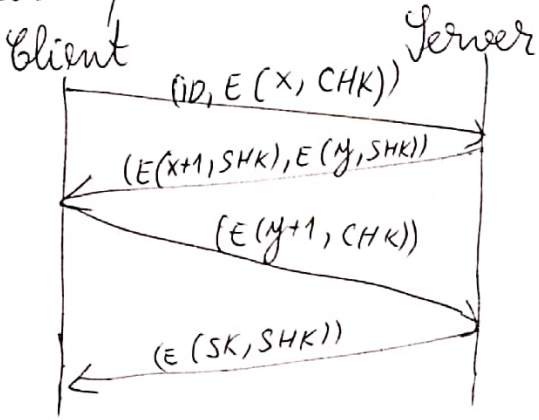
- Un proces x are cheia de decriptare (d_x, n_x) și cheia de criptare (e_x, n_x). La nivelul lui x avem:
1. p, q 2 nr. prime mari, $n = p * q$
2. d nr. întreg care este prim în raport cu $(p-1)*(q-1)$
3. se determină e nr. întreg, care este inversul lui $\boxed{d \% ((p-1)*(q-1))}$, adică $\boxed{e * d = 1 \% ((p-1)*(q-1))}$

- RSA poate fi folosit în criptarea/decriptarea oricărui mesaj
Dacă $p=5, q=11 \Rightarrow n=55$, $(p-1)*(q-1) = 40$. Alegem $d=23$ care este prim factor de 40. Rezultă ecuația $(23 * e) \% 40 = 1$
$\Rightarrow e = 7$

C10

Autentificarea

→ Autentificarea se ocupă cu pb. identificării exacte a procesului cu care se realizează comunicarea.
→ Autorizarea se ocupă cu cele ce îi este permis unui proces să facă în sistem.
→ Clientul trebuie să se asigure de identitatea serverului.
→ Autentificarea cu chei secrete:

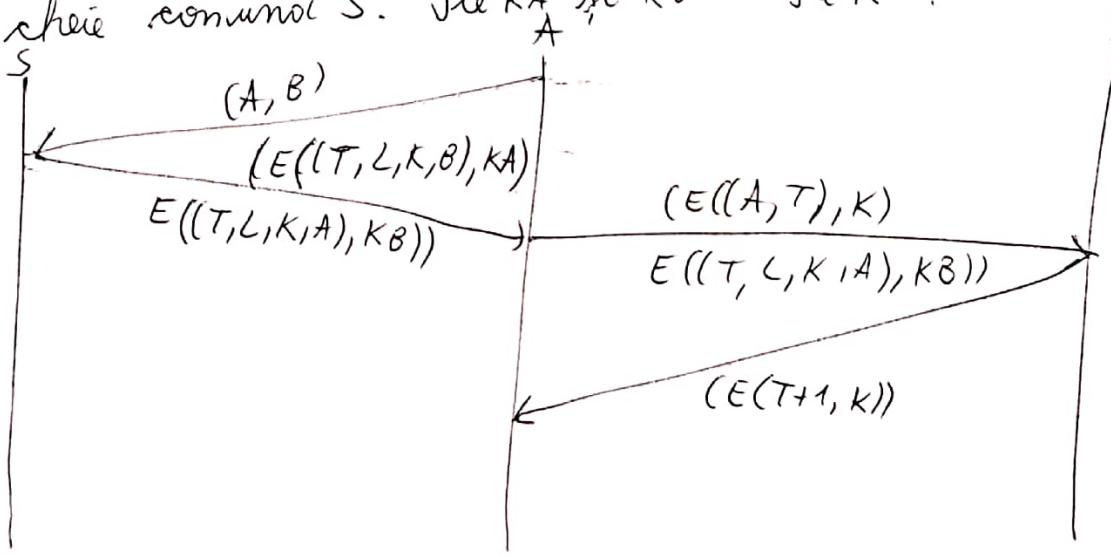


Clientul generează x random și îl criptează cu cheia secretă CKK, apoi trimite pe server mesajul E(X) CHK) împreună cu ID-ul său.

Serverul folosește cheia SHK asociată cu ID-ul clientului și trimite un mesaj cu un nr y generat random. Clientul decriptează mesajul.

→ Autentificarea cu chei publice

Sistemul de securizare bazat pe TCP/IP denumit Kerberos este cel mai utilizat. Considerând A și B doi participanți. Protocolul Kerberos presupune că A și B folosesc fiecare o cheie comună S. Fie KA și KB aceste KB.



Serverul generează o valoare a timpului T, un timp de viață L și o nouă cheie de sesiune K. Serverul S răspunde lui A, apoi A decriptează prima parte a mesajului, dar nu și pe cea de-a doua. A transmite partea a doua lui B, împreună cu criptarea lui A și T folosind cheia K. A a fost capabil să refacă pe L și T din decriptarea primei părți. B decriptează partea 2 și refac pe T, K, A, apoi va răspunde cu un mesaj care conține criptarea lui T+1 folosind cheia K.