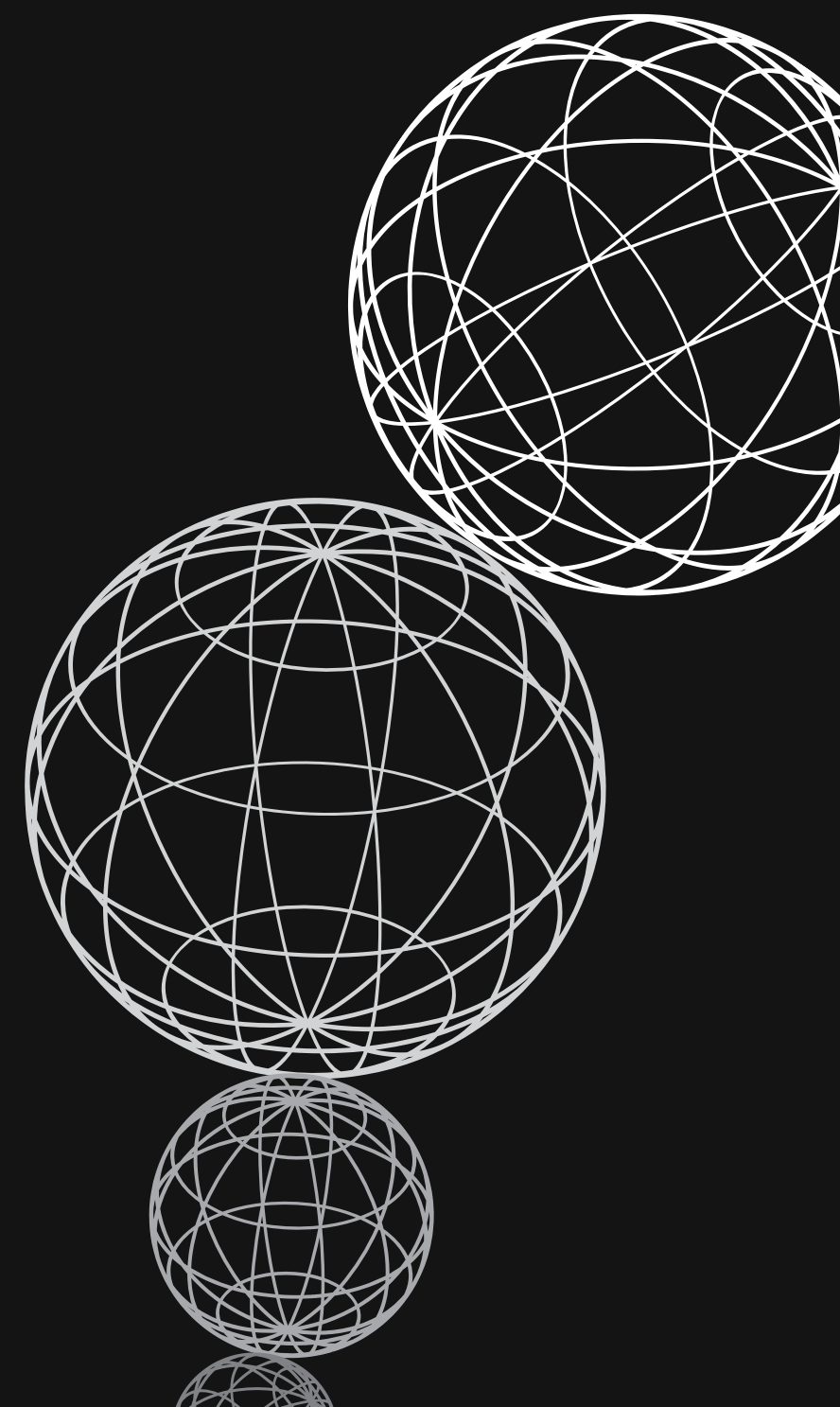


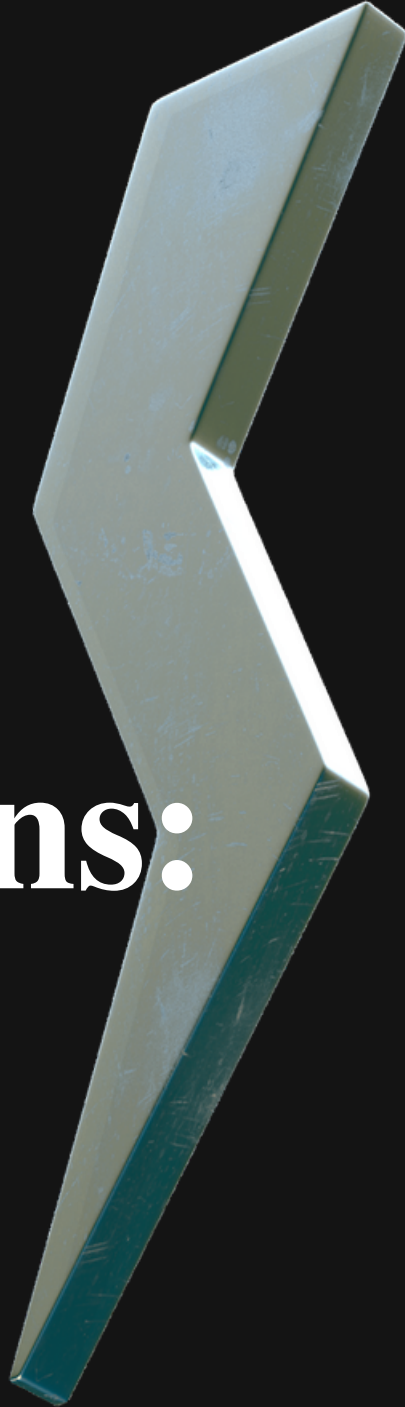
Rolul criptografiei in securitatea comunicatiilor

Elaborat: VICHILU ELENA
studenta grupei IT11Z
profesor: SKUTNITKI OLESEA



Criptografia

Cuprins:



Ce este necesar de stiut?

Ce este criptografia?

Definiții de bază

Cerințe pentru sistemele de protecție a informațiilor criptografice:

Scopul unui sistem criptografic

Criptarea: definiție și metode

Sarcinile criptografiei:

Concluzie



Ce este criptografia?



este știința care se ocupă cu studiul codurilor și cifrurilor. Un cifru este de fapt un algoritm criptografic care poate fi folosit pentru a transforma un mesaj clar (text clar) într-un mesaj indescifrabil (text cifrat). Acest proces de transformare se numește criptare iar procesul invers se numește decriptare. Textul cifrat poate fi transmis ulterior prin orice canal de comunicații fără a ne face griji că informații sensibile ar putea ajunge în mâinile inamicilor.

Definiții de bază

- Cifrare - un set de moduri predeterminate de a converti mesajul secret original pentru a-l proteja. • Un simbol este orice caracter, inclusiv o literă, un număr sau un semn de punctuație.
- Alfabet - un set finit de simboluri utilizate pentru a codifica informații.
- Mesaj criptat (criptogramă) - un mesaj primit după conversie folosind orice cifru.
- Cheie - informații necesare pentru criptarea și decriptarea mesajelor.
- Un sistem de criptare este orice sistem care poate fi utilizat pentru a modifica în mod reversibil textul unui mesaj pentru a-l face de neînțeles pentru oricine, în afară de destinatarul vizat.
- Rezistența criptografică - o caracteristică a unui cifru care determină rezistența acestuia la decriptare fără a cunoaște cheia (adică, capacitatea de a rezista criptoanalizei).
- Semnătură electronică (digitală) - un bloc de date atașat de obicei unui mesaj, obținut prin transformarea criptografică; O semnătură electronică permite unui alt utilizator să verifice paternitatea și autenticitatea mesajului la primirea textului.
- Sistem de securitate a informațiilor criptografice – un sistem de securitate a informațiilor care utilizează metode criptografice pentru a cripta datele.

Cerințe pentru sistemele de protecție a informațiilor criptografice:



UN MESAJ CRIPTAT TREBUIE SĂ
FIE LIZIBIL NUMAI DACĂ CHEIA
ESTE PREZENTĂ

CUNOAȘTEREA ALGORITMULUI
DE CRIPTARE NU AR TREBUI SĂ
AFECTEZE FIABILITATEA
PROTECȚIEI

ORICE CHEIE DIN SETUL DE
POSIBILE TREBUIE SĂ OFERE O
PROTECȚIE FIABILĂ A
INFORMAȚIILOR

ALGORITMUL DE CRIPTARE
TREBUIE SĂ PERMITĂ
IMPLEMENTAREA ATÂT
SOFTWARE CÂT ȘI HARDWARE



Scopul unui sistem criptografic

este de a cripta un text simplu semnificativ, rezultând un text cifrat (criptogramă) cu aspect complet lipsit de sens.

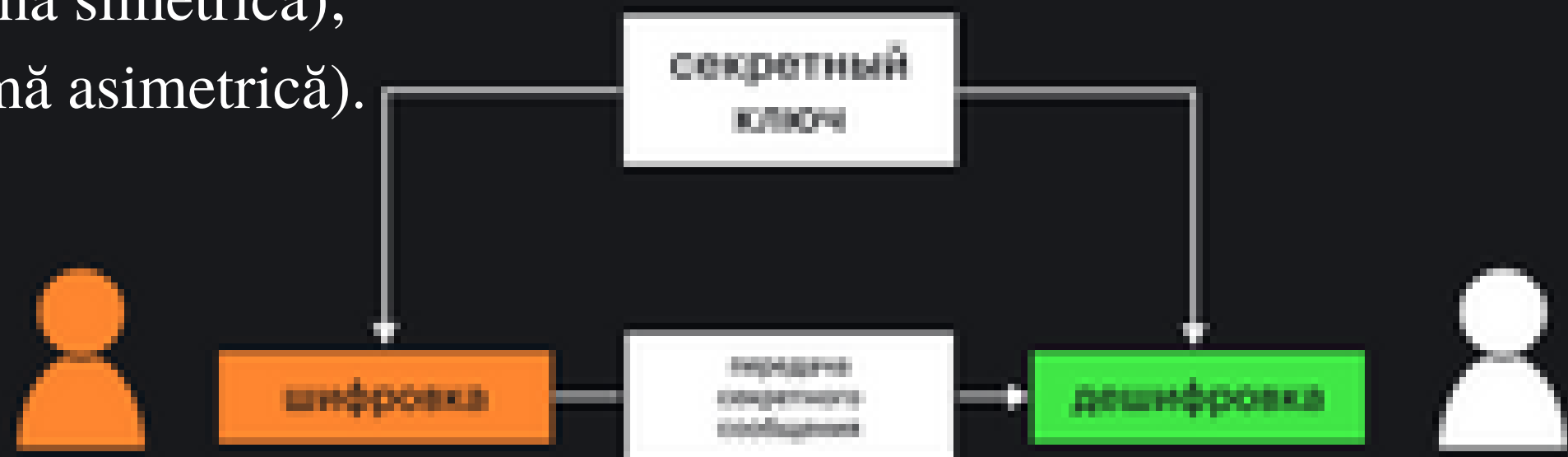
Destinatarul vizat trebuie să poată decripta („decripta”) acest text cifrat, restabilind astfel textul simplu corespunzător. În acest caz, adversarul (criptanalistul) trebuie să nu poată dezvălui textul sursă.

Criptarea: definiție și metode

Criptarea este o modalitate de a converti informații deschise în informații închise și invers. Este folosit pentru a stoca informații importante în surse nesigure sau pentru a le transfera prin canale de comunicare nesigure. Criptarea este împărțită în procesul de criptare și decriptare.

Metode de criptare:

- cifrări cu cheie secretă (schemă simetrică);
- cifruri cu cheie publică (schemă asimetrică).



Principalele direcții de criptare:



Criptarea datelor pe sistemele de discuri locale (criptare client)



Algoritm criptografic (cifrare) – un mod matematic specific și specific de prelucrare a informațiilor pentru a ascunde conținutul și sensul acesteia.

Principalele direcții de criptare:



Criptarea fișierelor individuale



Criptarea secțiunilor individuale de pe hard disk, unități virtuale

Sarcinile criptografiei:

CRIPTAREA EFECTIVĂ
A DATELOR PENTRU A
PROTEJA ÎMPOTRIVA
ACCESULUI
NEAUTORIZAT

AUTENTIFICARE
MESSAGE

VERIFICAREA
INTEGRITĂȚII
DATELOR TRANSMISE

NEREPUDIAREA

Domenii de aplicare a criptografiei:

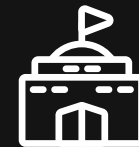
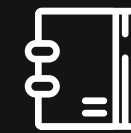
criptarea datelor în timpul transmiterii prin canale de
comunicație deschise;

serviciu de carduri bancare din plastic;

stocare și procesare a parolelor utilizatorului în rețea;

livrarea de rapoarte contabile și alte rapoarte prin canale de
comunicare la distanță;

servicii banking pentru întreprinderi printr-o rețea locală
sau globală; vsafe de acces neautorizat stocarea datelor pe
hard disk-ul computerului (sistem de fișiere criptate EFS);



După ce am studiat materialul despre criptografie, putem concluziona că, de fapt, totul funcționează mult mai complicat decât credem inițial. Evoluția criptografiei și criptoanalizului arată că omenirea a început inventarea acestor sisteme din structuri primitive, iar astăzi avem modele destul de complexe și bine gândite.

