CRIPTOGRAFIE ȘI SECURITATE

Curs opțional – anii III și IV CTI

Conf.univ.dr. Radu Boriga

- Scurt istoric al criptografiei
- Cifruri de substituție monoalfabetice și polialfabetice
- Cifruri de permutare
- Principiile criptografiei moderne
- Primitive criptografice moderne
- Generatoare de numere pseudoaleatoare
- Criptografia bazată pe haos

- **Nota laborator (40% - fără prag minim)**
- **Examen (60% - minim nota 5)**

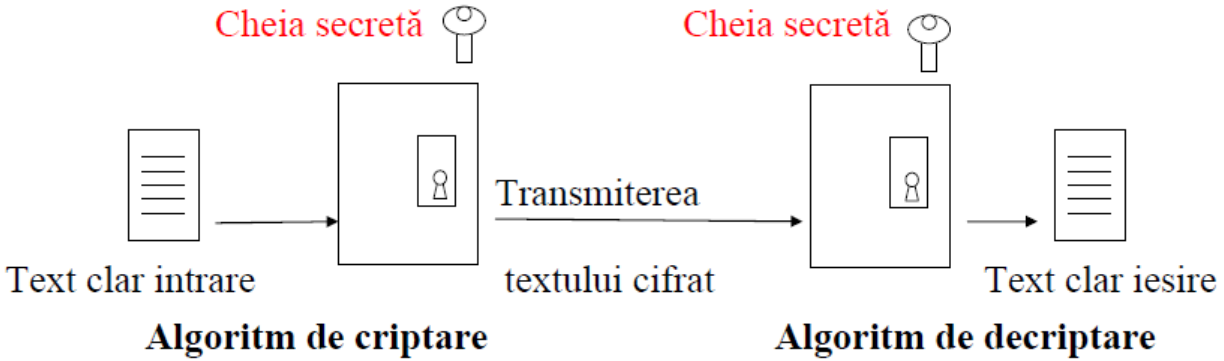
- **Examenul va fi diferențiat pentru anii III și IV!**

BIBLIOGRAFIE

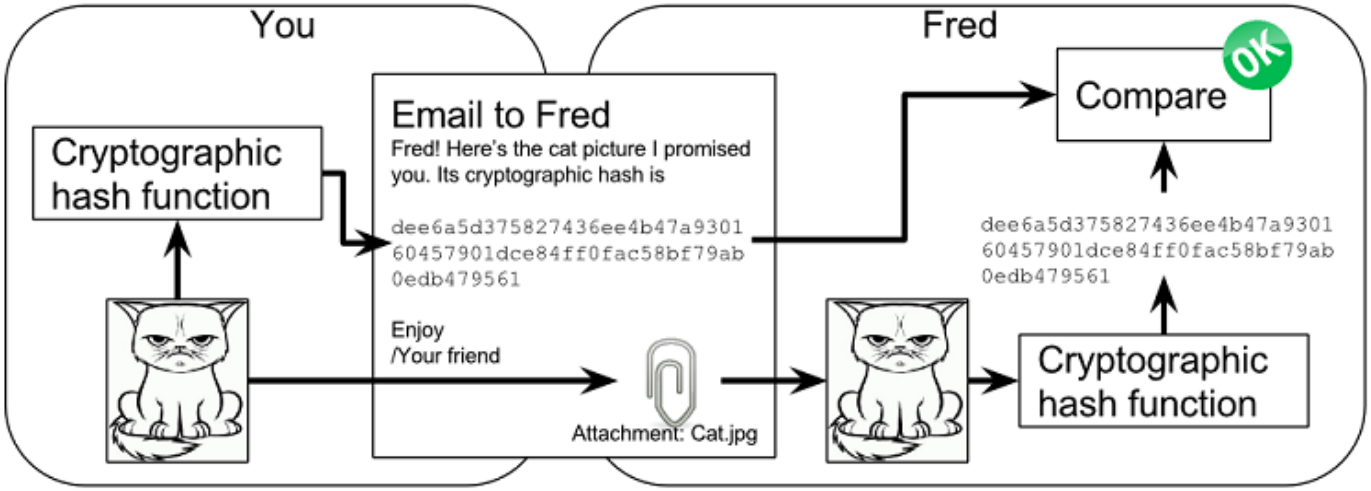
- Adrian Atanasiu, "Curs de criptografie (semestrul I)", http://www.galaxyng.com/adrian_atanasiu/cript.htm
- Adrian Atanasiu, "Securitatea Informației. Criptografie (volumul I)", Ed. Infodata Cluj, 2007
- Bruce Schneier, "Applied Cryptography", Wiley & Sons, 1996
- Alfred Menezes, Paul van Oorschot, Scott Vanstone, "Handbook of Applied Cryptography", CRC Press, 2001

- Combinatorică
- Algebra câmpurilor finite
- Teoria numerelor
- Teoria curbelor eliptice
- Probleme NP-complete
- Teoria haosului
- Mecanică cuantică

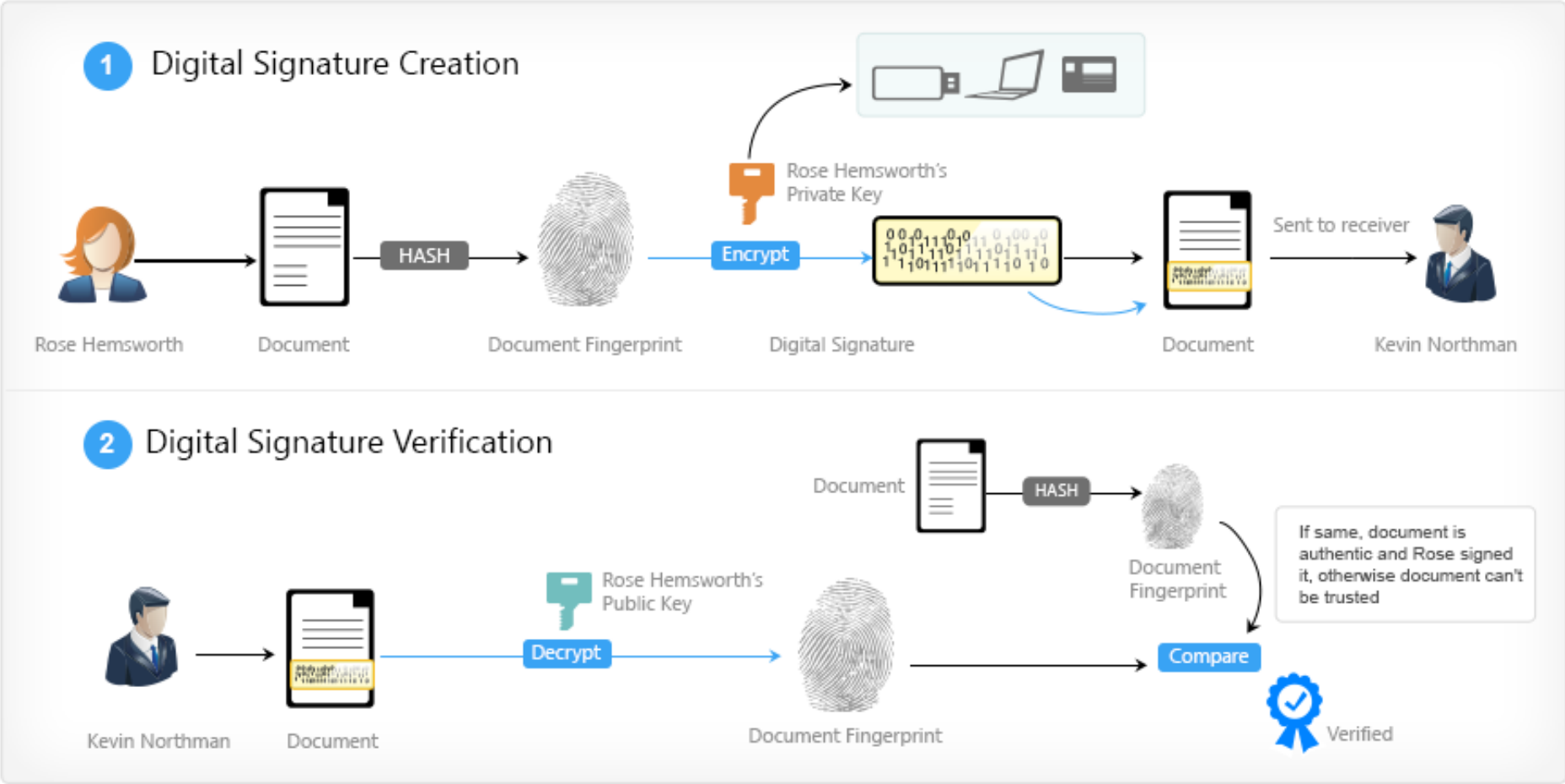
➢Sisteme de criptare



➢Funcții criptografice pentru hash



➢Semnături digitale



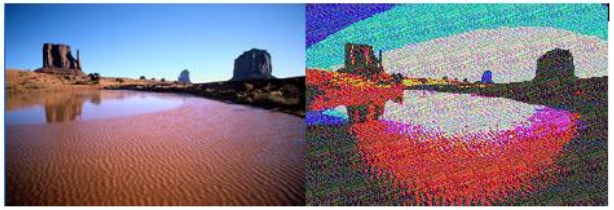
➢Steganografie

decode → Bob stole the bank

Hidden message

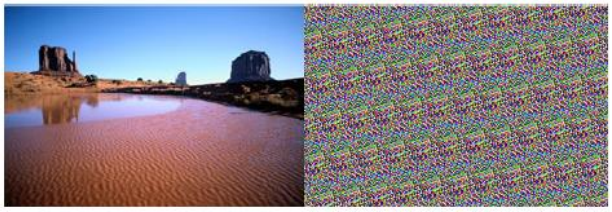
Image B

4 LSB modified produces banding



7 bits

6 bits

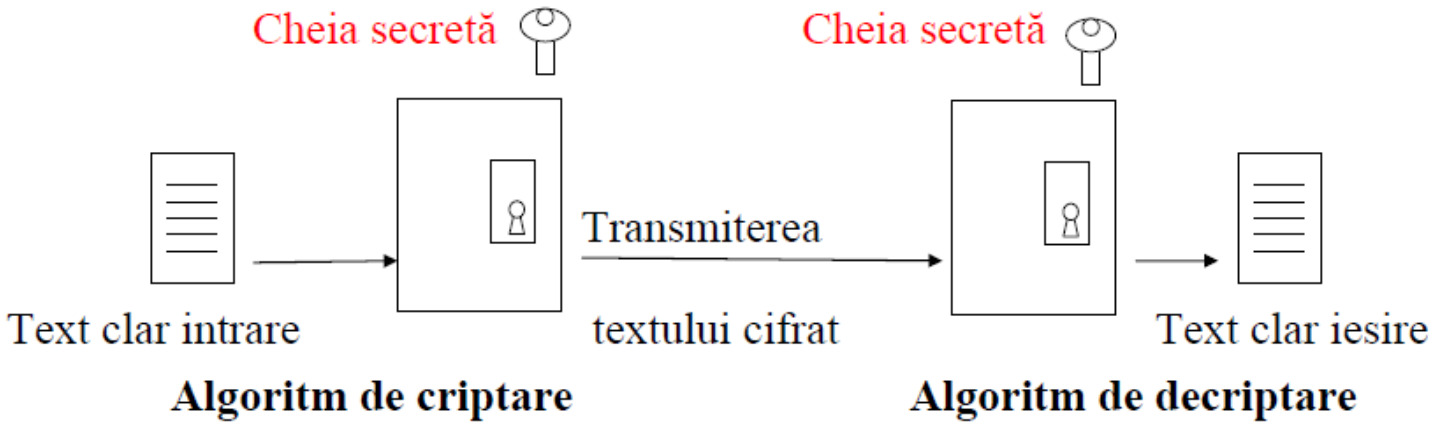


All 8 bits

➢ Watermarking

- Cuvântul **criptografie** provine din limba greacă: *kryptós* (ascuns) și *gráfein* (a scrie).

Cryptography is the art of keeping secret a secret...



➢ Perioada antică:

- **Scitala** – cifru de transpoziție care folosea un cilindru pe care era înfășurată o bandă de pergament pe care se scria textul clar, după care banda era desfășurată

- **Cifrul lui Cezar** – cifru de substituție monoalfabetic

➢ Perioada medievală:

- **Codul lui Alberti** – primul cifru de substituție polialfabetic inventat în 1467 de către *Leon Battista Alberti*

- **Cifrul Vigenère** – cifru de substituție polialfabetic cu cheie secretă inventat în 1553 de către *Giovan Battista Bellaso*, dar atribuit, în mod eronat, lui *Blaise de Vigenère* care în 1586 a inventat un sistem de cifrare asemănător

➢ **Perioada modernă:**

- **Principiile lui Kerckhoffs** – au fost formulate în 1883 de către *Auguste Kerckhoffs* și precizează condițiile pe care trebuie să le îndeplinească un sistem de criptare pentru a fi considerat sigur. Cel mai cunoscut dintre ele este următorul: "*Un sistem de criptare trebuie să fie sigur chiar și în cazul în care se cunosc toate detalii despre el, mai puțin cheia secretă*."

- **Cifrul lui Vernam** – un sistem de criptare fluid, singurul având securitate necondiționată, inventat în 1918 de către *Gilbert Sandford Vernam*

- **Mașina Enigma** – a fost construită în 1919 de *Arthur Scherbius*, pe baza unui cifru de substituție polialfabetic complex, și utilizată de către germani în cel de-al II-lea Război Mondial

- **Principiile lui Shannon** – au fost formulate în 1948 de către *Claude Shannon* și postulează condițiile pe care trebuie să le îndeplinească un sistem de criptare pentru a fi sigur pe baza noțiunilor de *difuzie* și *confuzie*.

➢ Principiul lui Kerckhoffs:

- *"Only the key should be secret, not the algorithm."*

➢ Principiile lui Shannon:

- **Difuzie:** *"The statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext."*
- **Confuzie:** *"Attempts to make the relationship between the ciphertext and the key as complex as possible."*

A SIMPLE EXAMPLE

PERMUTARE

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 9 & 7 & 1 & 13 & 10 & 8 & 6 & 11 & 15 & 4 & 14 & 16 & 3 & 5 & 12 & 2 \end{pmatrix}$$

SEMEPL PAMELIX A

SUBSTITUȚIE

Fiecare literă este deplasată cu trei poziții către dreapta

VHPHSO SDPHOLA D

➢ Perioada contemporană:

- **Protocolul Diffie-Hellmann** – pentru distribuția cheilor publice, inventat în 1976 de *Whitfield Diffie* și *Martin Hellman*
- **Sistemul de criptare RSA** – sistem asimetric de criptare cu cheie publică, care poate utilizat atât pentru criptare, cât și pentru semnătura electronică, propus în 1978 de *Ron Rivest*, *Adi Shamir* și *Leonard Adleman*.
- **Sistemul de criptare DES** - un sistem de criptare selectat ca standard federal de procesare a informațiilor în Statele Unite în 1976, în prezent fiind considerat nesigur.
- **Sistemul de criptare AES** - un sistem de criptare simetric pe blocuri standardizat în 2001 de NIST pentru protecția datelor electronice, inventat de către *Joan Daemen* și *Vincent Rijmen*
- **Criptografia bazată pe sisteme dinamice haotice** - în 1998, Murilo Da Silva Baptista a propus primul algoritm de criptare care folosea în mod explicit caracteristici specifice doar sistemelor dinamice discrete haotice

- **Obiectivele criptografiei:**
  - **Confidenţialitatea:** informaţia rămâne accesibilă doar părţilor autorizate
  - **Integritatea datelor:** proprietatea de a detecta orice modificare (inserare, ștergere, substituție) neautorizata a informației
  - **Autentificare:** proprietatea de a identifica sursa unei anumite informații
  - **Non-repudierea:** proprietatea care previne negarea unor evenimente efectuate anterior

- **Criptologia** este ştiinţa care se ocupă cu studiul comunicaţiilor sigure şi cuprinde **criptografia** și **criptanaliza**.

- **Criptografia** este studiul metodelor matematice legate de securitatea informației, capabile să asigure confidențialitatea, autentificarea şi non-repudierea mesajelor, precum și integritatea datelor vehiculate.

- O **schemă de criptare** convenţională este alcătuită din cinci elemente:
  - **Textul clar:** mesajul original sau informaţia de intrare pentru algoritmul de criptare
  - **Algoritmul de criptare:** un algoritm care execută diferite substituţii şi transformări asupra textului clar
  - **Cheia secretă:** dată de intrare pentru algoritmul de criptare.
  - **Textul cifrat:** textul rezultat după aplicarea algoritmul de criptare, dependent de textul clar şi de cheia secretă;
  - **Algoritmul de decriptare:** algoritmul invers celui de criptare, fiind aplicat textului cifrat şi aceleaşi chei secrete pentru a obţine textul clar original.
- Pentru un mesaj dat, două chei secrete diferite produc două texte cifrate diferite.
- **Criptanaliza** este ramura criptologiei care se ocupă cu spargerea cifrurilor pentru refacerea informaţiilor.
- Un criptosistem este considerat sigur dacă obţinerea textului clar plecând de la textul cifrat, fără a cunoaşte cheia secretă, este o problema cu grad înalt de dificultate din punct de vedere computațional.