CRYPTOLOGY

from theory to practice

EMIL SIMION, Ph.D.

e-mail: esimion@fmi.unibuc.ro; esimion@upb.ro

AGENDA

I. Introduction to information security (models of security);

II. Cryptology: cryptography and cryptanalysis;

III. Course profile;

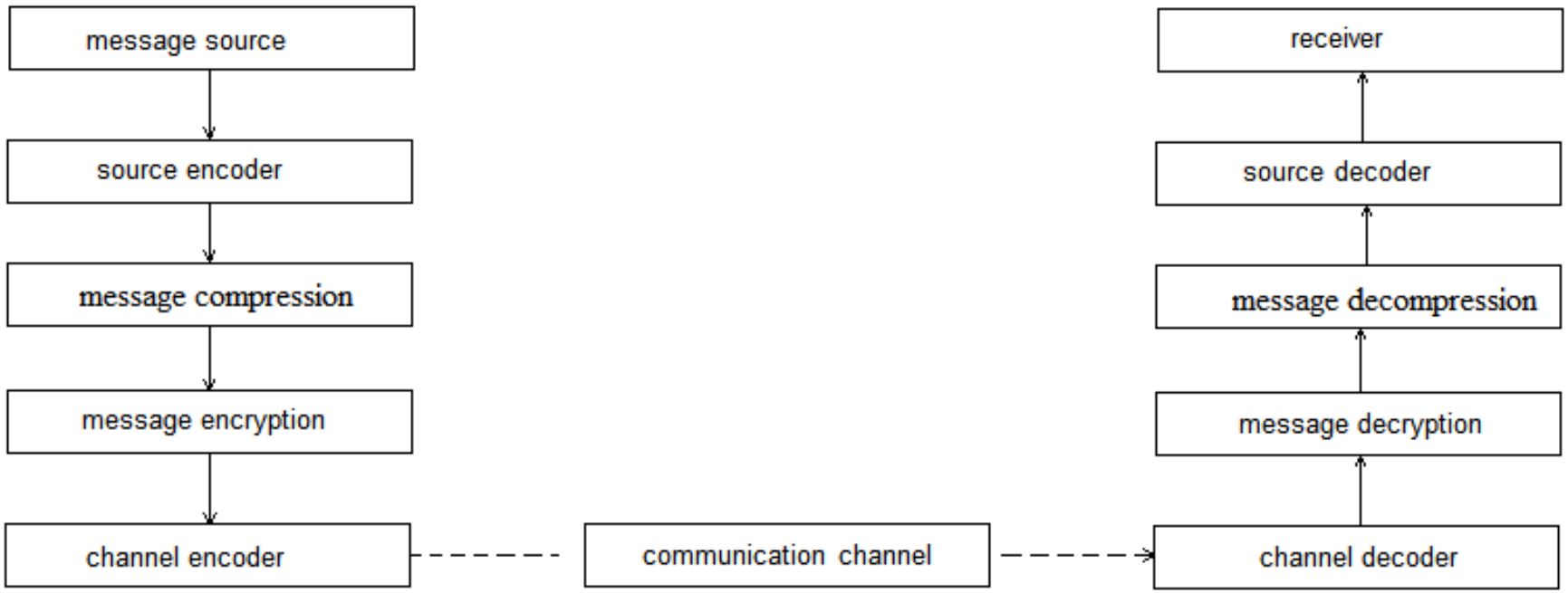
IV. References;

V. Examination.

I. Shannon model for information transmission

- **Claude Elwood Shannon** (April 30, 1916 – February 24, 2001) published, in 1949, *Communication Theory of Secrecy Systems* discussing cryptography from the viewpoint of information theory.

Shannon model for information transmission - cont

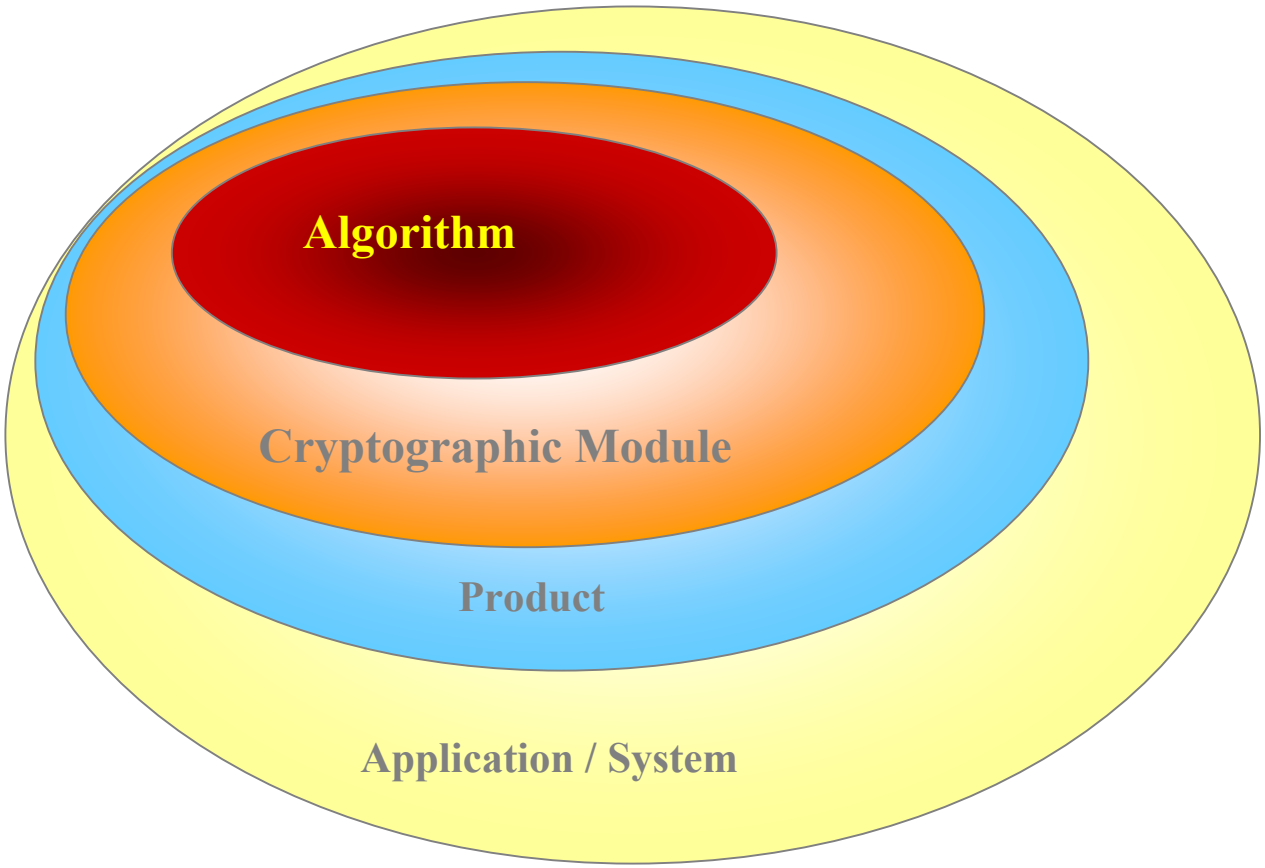


Information security attributes

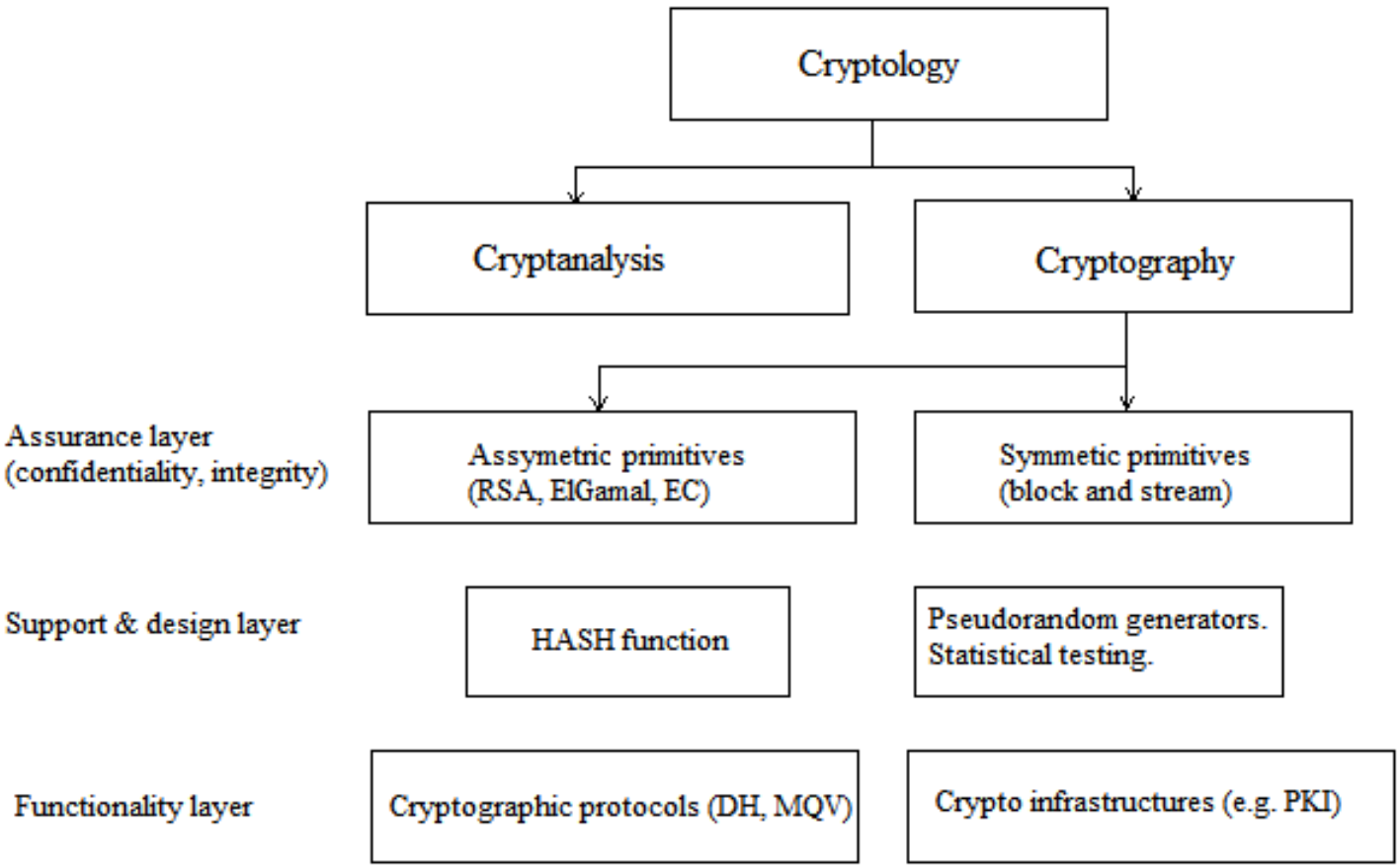
- Confidentiality;
- Integrity;
- Authenticity;
- Non-repudiation;
- Availability.

Model for security

Cryptographic algorithms are mathematical objects used in cryptographic modules (software, firmware and/or hardware) . These **crypto-modules** are used to **design cryptographic products** (applications and/or devices). The cryptographic products are used to protect data in **communication systems** or in **specific applications**.



II. Cryptology

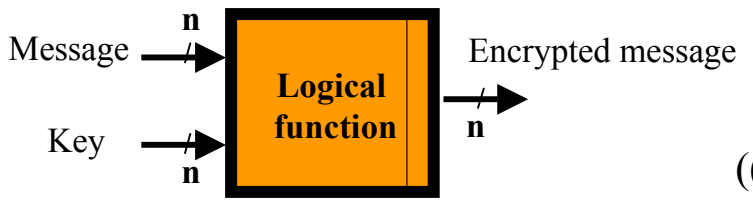


Some example: crypto algorithms

- Cryptographic algorithms ensure: **confidentiality** and **integrity** (authentication, non repudiation and protection against errors) of the data;
- Two type of algorithms: **asymmetric** (two different keys, one for encryption another for decryption, based on the computational difficulty of several problems: e.g. RSA [factoring], ElGamal [discreet log problem] and their extension to Elliptic curves) and **symmetric** (the same key used for encryption and decryption, e.g. AES).

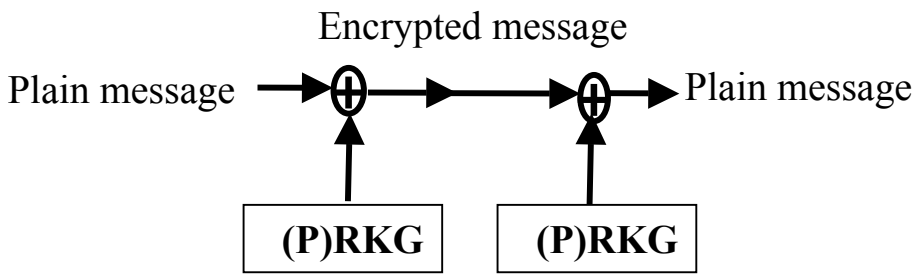
Symmetric ciphers: block and stream

Block cipher
No internal state

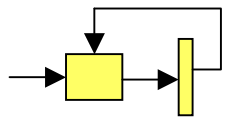


Stream ciphers
Internal state

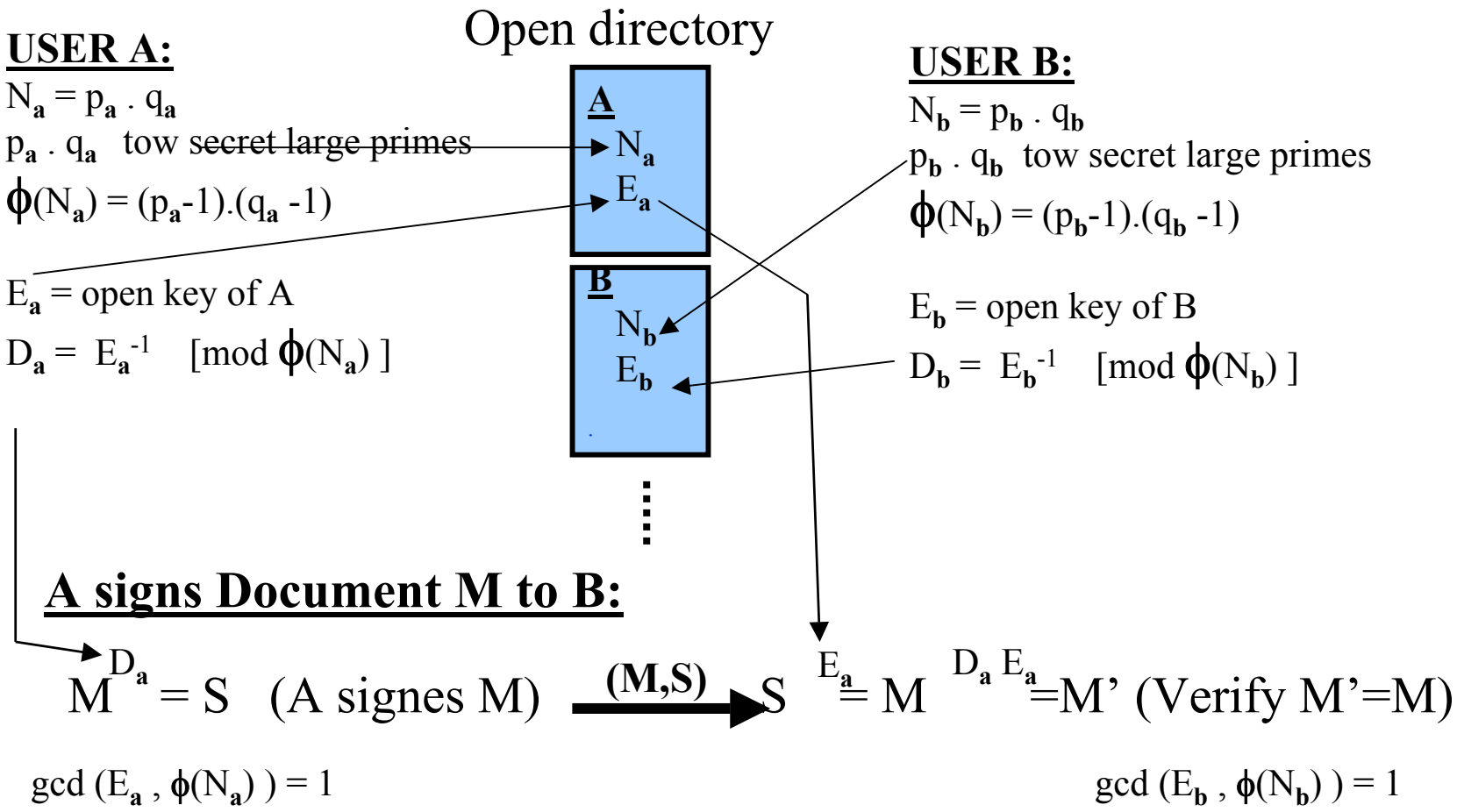
Additive stream cipher
((Pseudo)random key generator
(P)RKG)



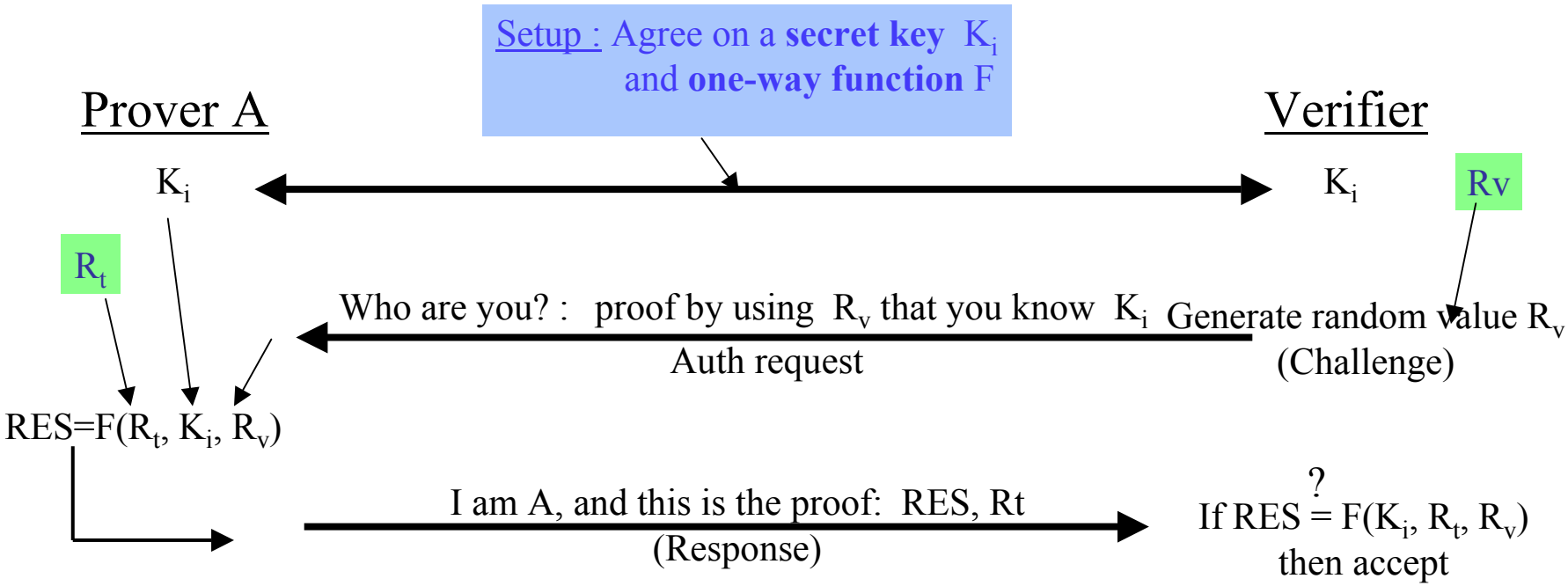
General stream cipher



Asymmetric ciphers: example RSA



Practical example: Challenge-Response Identification Mechanism



Course profile

- **Classic ciphers**: Cesar, substitutions, Playfair, Hill, polyalphabetic,transpositions, mixed systems;
- **Statistics**: estimation and statistical tests;
- **Algebra**: Computation in Galois field, Chinese Remainder Theorem etc.;
- **Pseudorandom generators**;
- **Symmetric ciphers**: AES candidate ciphers;
- **Asymmetric ciphers**: Merkle-Hellmann, RSA, ElGamal, EC;
- **Cryptographic protocols**: Diffie-Hellmann;
- **Cryptousage** (PKI, e-mail security, IPSEC etc.);
- **Evaluation** *versus* **cracking**.

References

- J. Menezes and P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, fifth edition, ISBN 9780849385230, 2001.
- B. Scheneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Second Edition, ISBN 0-471-12845-7, 1996.
- D. Naccache and E. Simion, *Information security and Cryptology. Applications*, MATRIX ROM, ISBN 978-973-755-675-2 , 2011.
- D. Stinson, *Cryptography Theory and Practice*, CRC Press, Third edition, ISBN 9781584885085, 2005.

Examination

- **H**omework project;
- **A**pplication project you can work in a team of max. 4 members;
- **S**eminar activity (bonus points);
- **F**inal test (with computers support): 2 hours.
- Final mark: (**H**+**A**+**F**)/3 + **S**.
- Proposals?

Thank you for your attention!