Course Plan

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

January 05, 2021

Course Details

Course	:	Institute Elective
Title	:	Cryptography
Instructor	:	Dr. Odelu Vanga

Textbook:

- **Cryptography and Network Security**, Behrouz A Forouzan, Debdeep Mukhopadhyay, McGraw-Hill Education, 2011.
- **Cryptography: Theory and Practice** by Douglas Stinson, 3/e, 2006.

Course Details

Course : Institute Elective
Title : Cryptography
Instructor : Dr. Odelu Vanga

Textbook:

- **Cryptography and Network Security**, Behrouz A Forouzan, Debdeep Mukhopadhyay, McGraw-Hill Education, 2011.
- **Cryptography: Theory and Practice** by Douglas Stinson, 3/e, 2006.

References:

- "Cryptography and Network Security: Principles and Practice", William Stallings, 6th Edition, Pearson Education, 2014.
- "A course in number theory and cryptography", Neal Koblitz, Second Edition, Springer.
- "Handbook of Applied Cryptography", Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, CRC Press.
- "Blockchain Technology Overview", D. Yaga, P. Mell, N. Roby, and K. Scarfone, NISTIR 8202.
- Classroom Lecture Notes

Evaluation Scheme

Component	Duration	Weightage(%)	Date & Time	Nature of Component
Mid-Sem Exam	–	20%	–	Closed Book
End-Sem Exam	–	30%	–	Closed Book
Scheduled Quiz	–	30%	–	Closed Book
CPQ*	–	10%	–	Closed Book
Term Project	–	10%	–	Open Book

CPQ*: Class Participation Quiz

Evaluation Scheme

Term Project Details

- It should submit one page report, includes title and tentative plan work on/before January 30, 2021.

Evaluation Scheme

Term Project Details

- It should submit one page report, includes title and tentative plan work on/before January 30, 2021.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary on/before March 20, 2021.

Evaluation Scheme

Term Project Details

- It should submit one page report, includes title and tentative plan work on/before January 30, 2021.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary on/before March 20, 2021.
- Final project report should submit with experimental results on April 10, 2021.

Evaluation Scheme

Term Project Details

- It should submit one page report, includes title and tentative plan work on/before January 30, 2021.
- Submit work implementation plan two pages, include abstract, experiments plan, and summary on/before March 20, 2021.
- Final project report should submit with experimental results on April 10, 2021.
- I will announce the project viva dates based on the available time slots.

Make-ups and Notices

Make-up policy

- No Make-ups for Term Project.
- Makeup for other components is granted on prior permissions as per institute policy.

Make-ups and Notices

Make-up policy

- No Make-ups for Term Project.
- Makeup for other components is granted on prior permissions as per institute policy.

Consultation and Notices

- Doubt clarification hours - Contact in Google classroom
- Notices/announcements regarding the course will be displayed in Google Classroom

Course Syllabus

Overview of Course Structure

M1: Number Theory Basics
Modular arithmetic, Primes, Euclidean Algorithm, Chinese Remainder Theorem.

M2: Shannon's Theory
Perfect Secrecy, Entropy, Security analysis of Classical ciphers.

M3: Symmetric Key Cryptography
DES, Finite Fields, AES, Security Analysis.

M4: Public Key Cryptography
RSA, ElGamal, Elliptic Curve Cryptography.

M5: Digital Signatures
Hash functions, Digital Signature Algorithm, ElGamal Digital Signature.

M6: Applications
Key Distribution, Diffie-Hellman Kay Exchange, Key Management in Distributed Systems.

History

Historical perspective

Before World War II (1940s)

- **"Secret writing"**
  - 1900 B.C. – non-standard methods
  - Julius Caesar

Historical perspective

Before World War II (1940s)

- **"Secret writing"**
  - 1900 B.C. – non-standard methods
  - Julius Caesar
- **Modern theory starts around the U.S. Civil War (1861-1865)**
  - Playfair

Historical perspective

Before World War II (1940s)

- **"Secret writing"**
  - 1900 B.C. – non-standard methods
  - Julius Caesar
- **Modern theory starts around the U.S. Civil War (1861-1865)**
  - Playfair
- **Extensive use of code books**
  - Telegrams and commercial codes
  - Vernam cipher

World War-I (lasted in 1914 - 1918)

Modern History

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**

Modern History

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
  - Data Encryption Standard (DES, 1977)
  - “New Directions in Cryptography” (1976)
    - Diffie and Hellman’s introduction of Public Key Cryptography

Modern History

After World War II (1940s)

- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
  - Data Encryption Standard (DES, 1977)
  - “New Directions in Cryptography” (1976)
    - Diffie and Hellman’s introduction of Public Key Cryptography
  - RSA (Rivest, Shamir, Adelman) (1977)
  - AES - 128 (2001)
  - ECC (1984)

Modern History

After World War II (1940s)

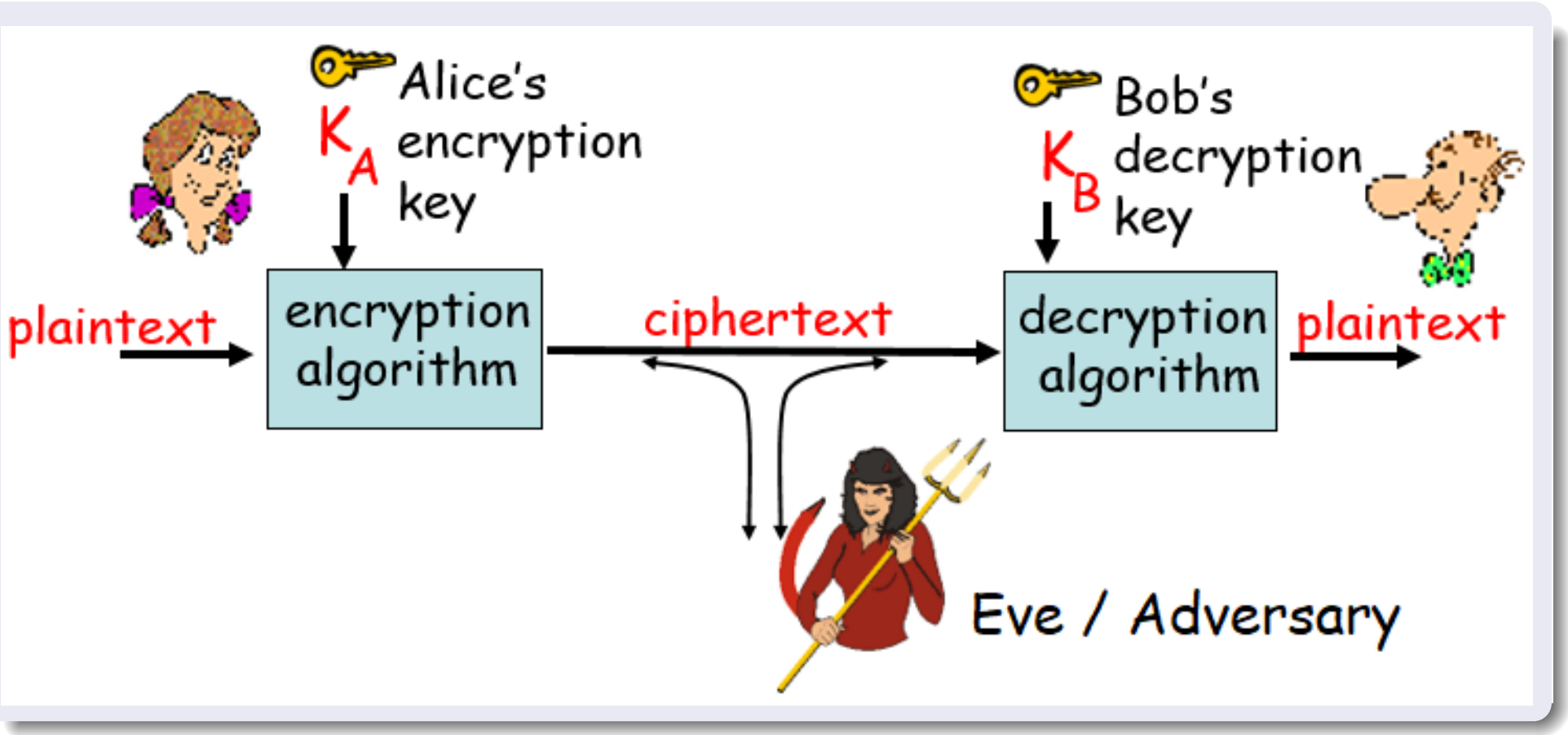
- **Claude Shannon and Information Theory (1948)**
- **1974, public interest resumes**
  - Data Encryption Standard (DES, 1977)
  - "New Directions in Cryptography" (1976)
    - Diffie and Hellman's introduction of Public Key Cryptography
  - RSA (Rivest, Shamir, Adelman) (1977)
  - AES - 128 (2001)
  - ECC (1984)

Hash Functions

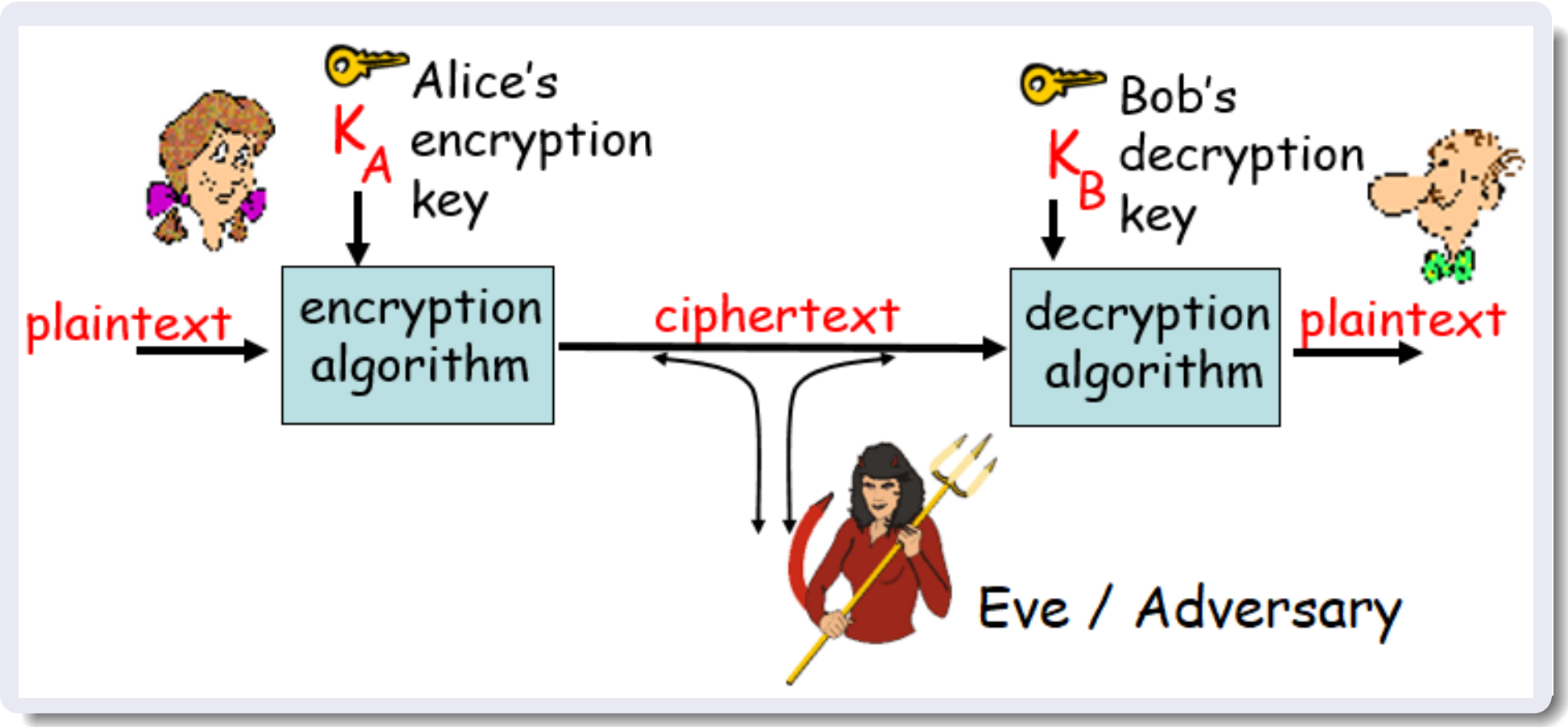
- First design of cryptographic hash function proposed in 1970s
- More proposals emerged in the 1980s

Introduction to cryptography

Message Communication

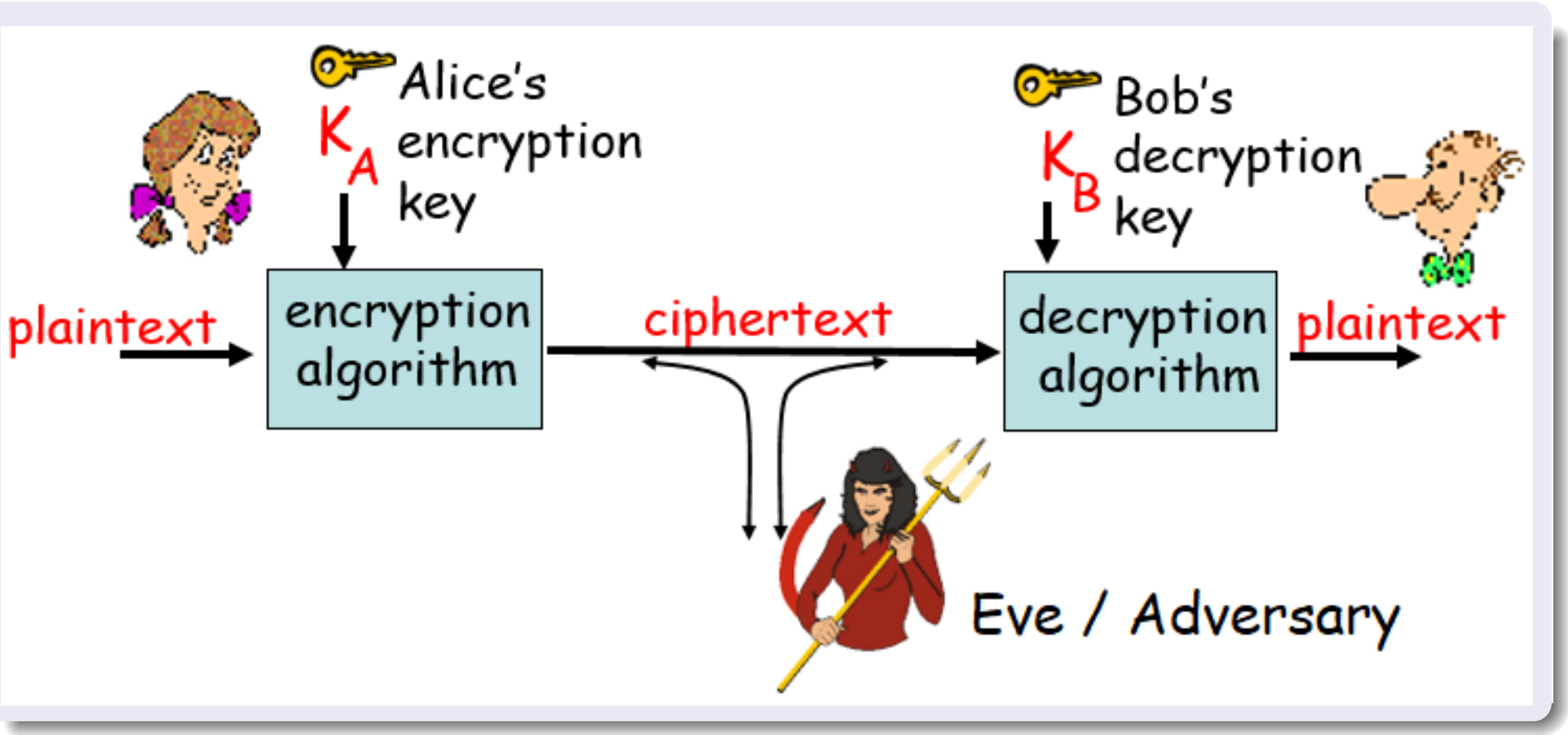


Message Communication



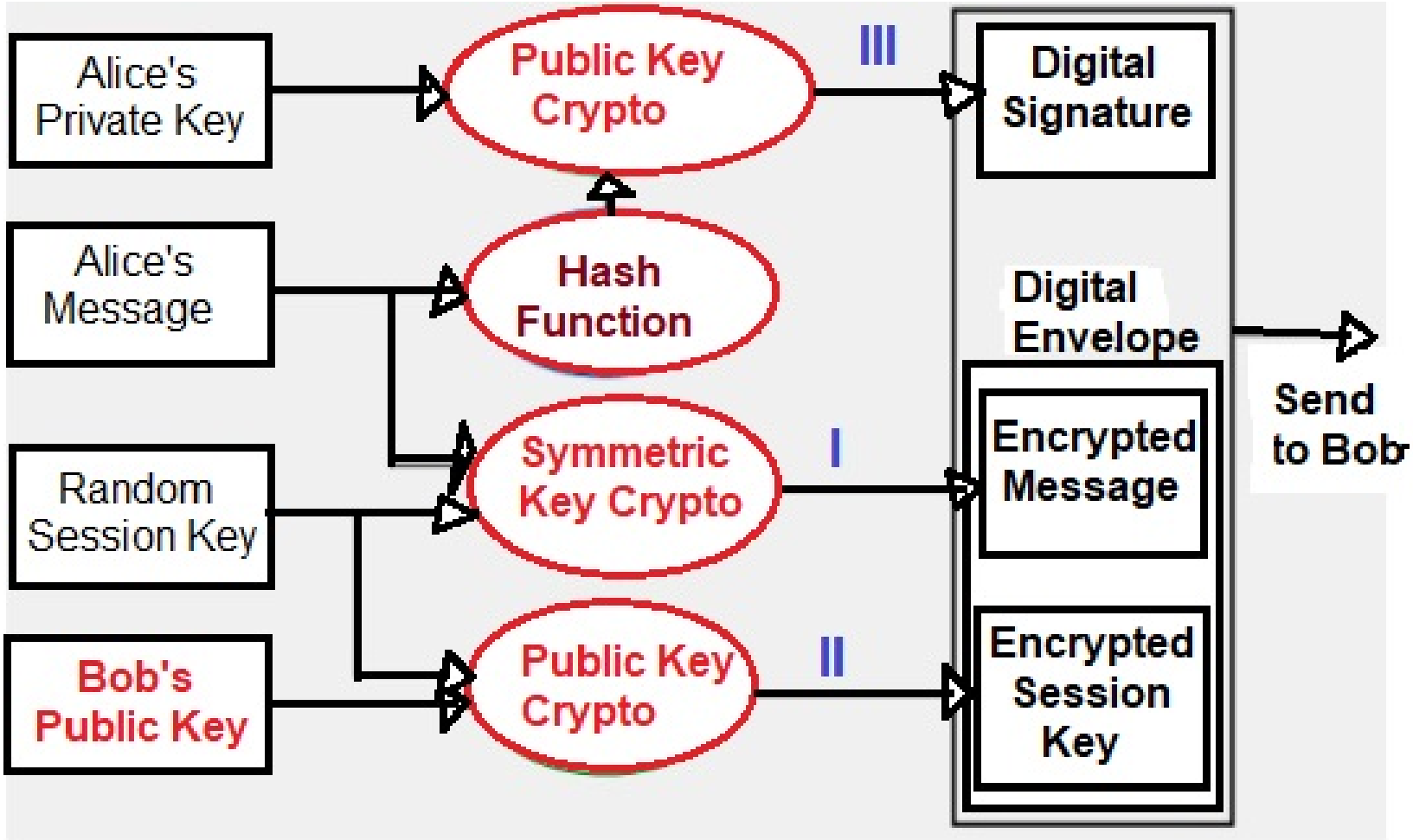
- **Symmetric-key cryptography**
  sender, receiver keys are identical, that is, $K_A = K_B$.

Message Communication

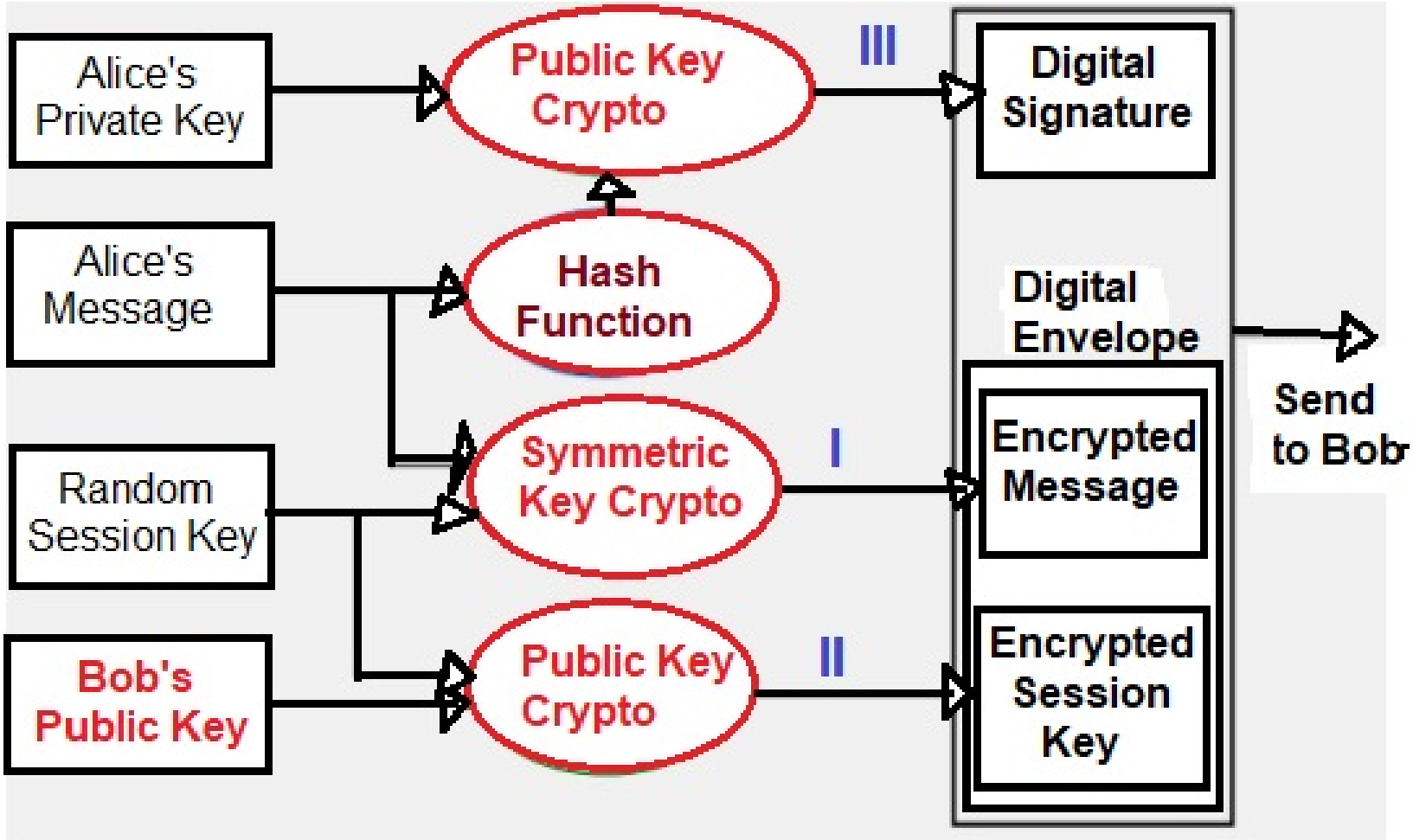


- **Symmetric-key cryptography**
  sender, receiver keys are identical, that is, $K_A = K_B$.
- **Asymmetric-key cryptography**
  encryption key (public), decryption key (private), that is, $K_A \neq K_B$.

Goals and Mechanisms

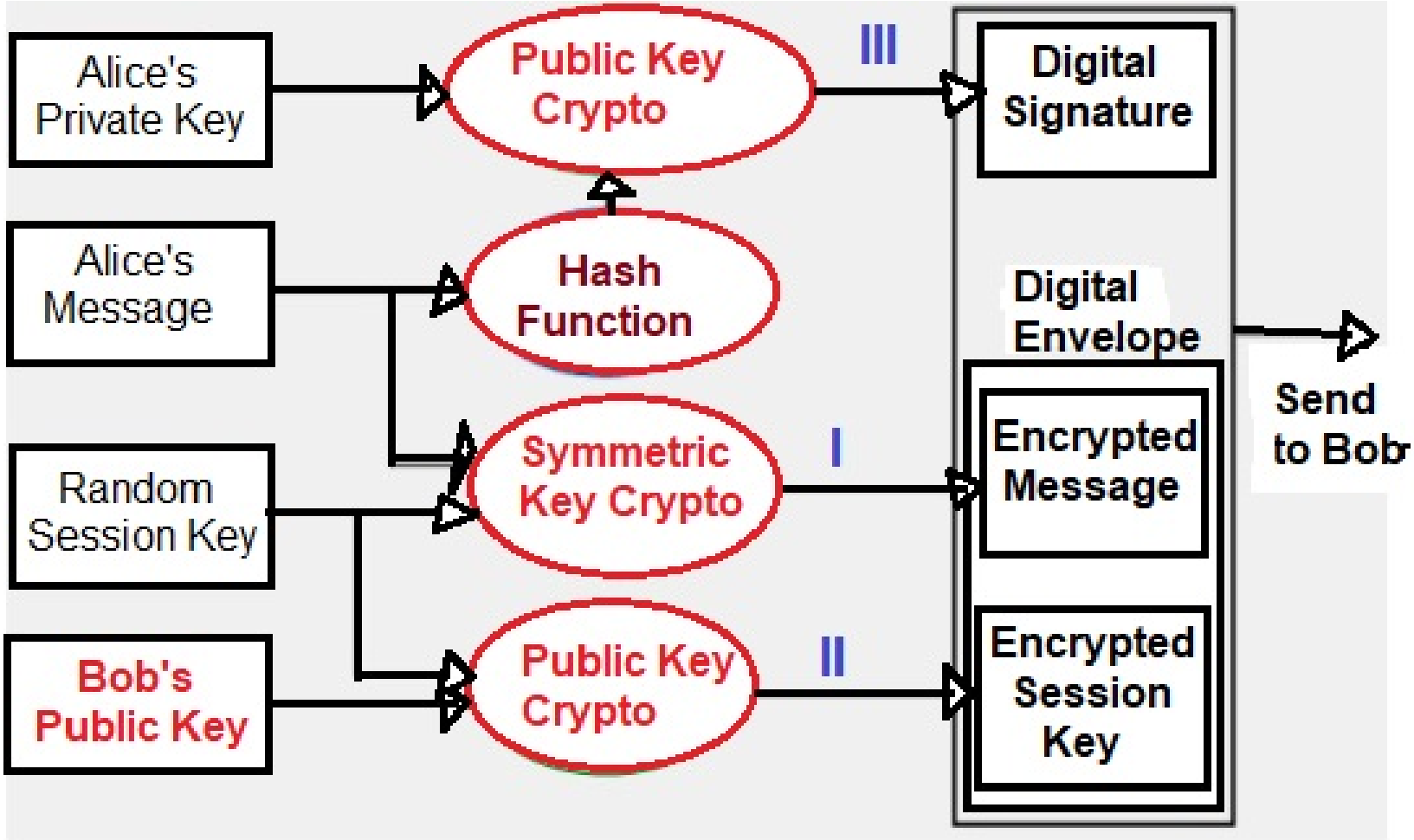


Goals and Mechanisms



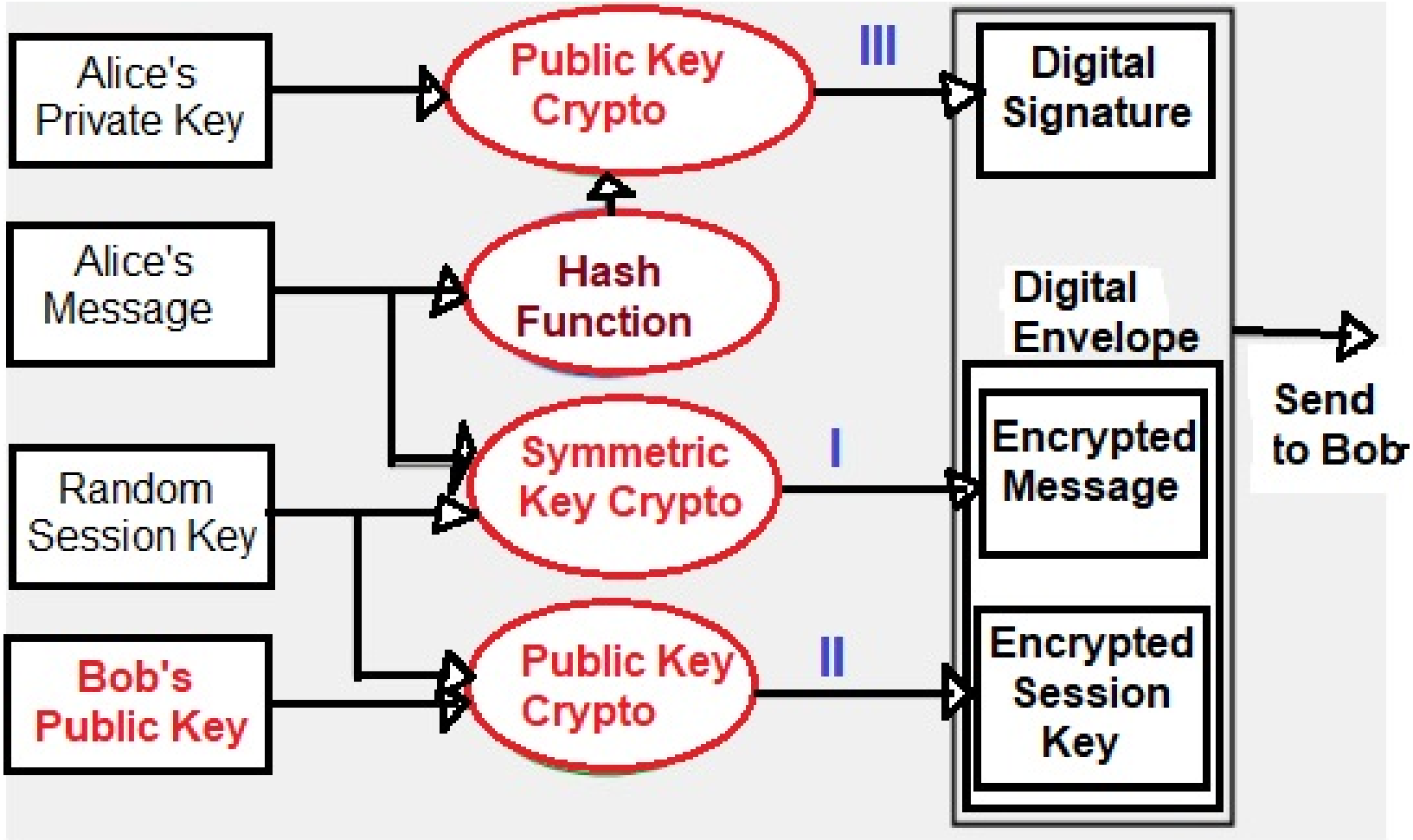
- **Confidentiality**

Goals and Mechanisms



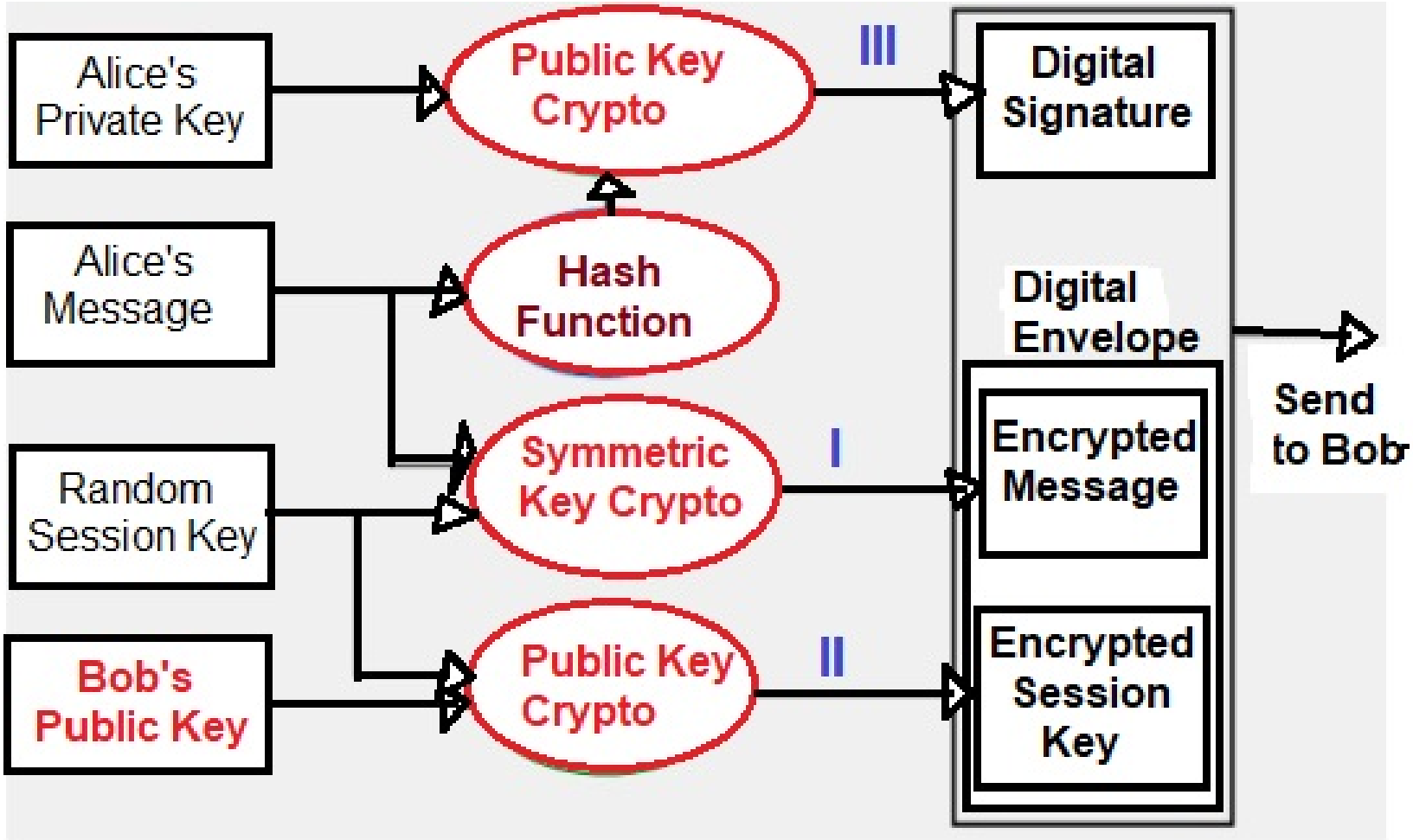
- **Confidentiality**
- **Integrity**

Goals and Mechanisms



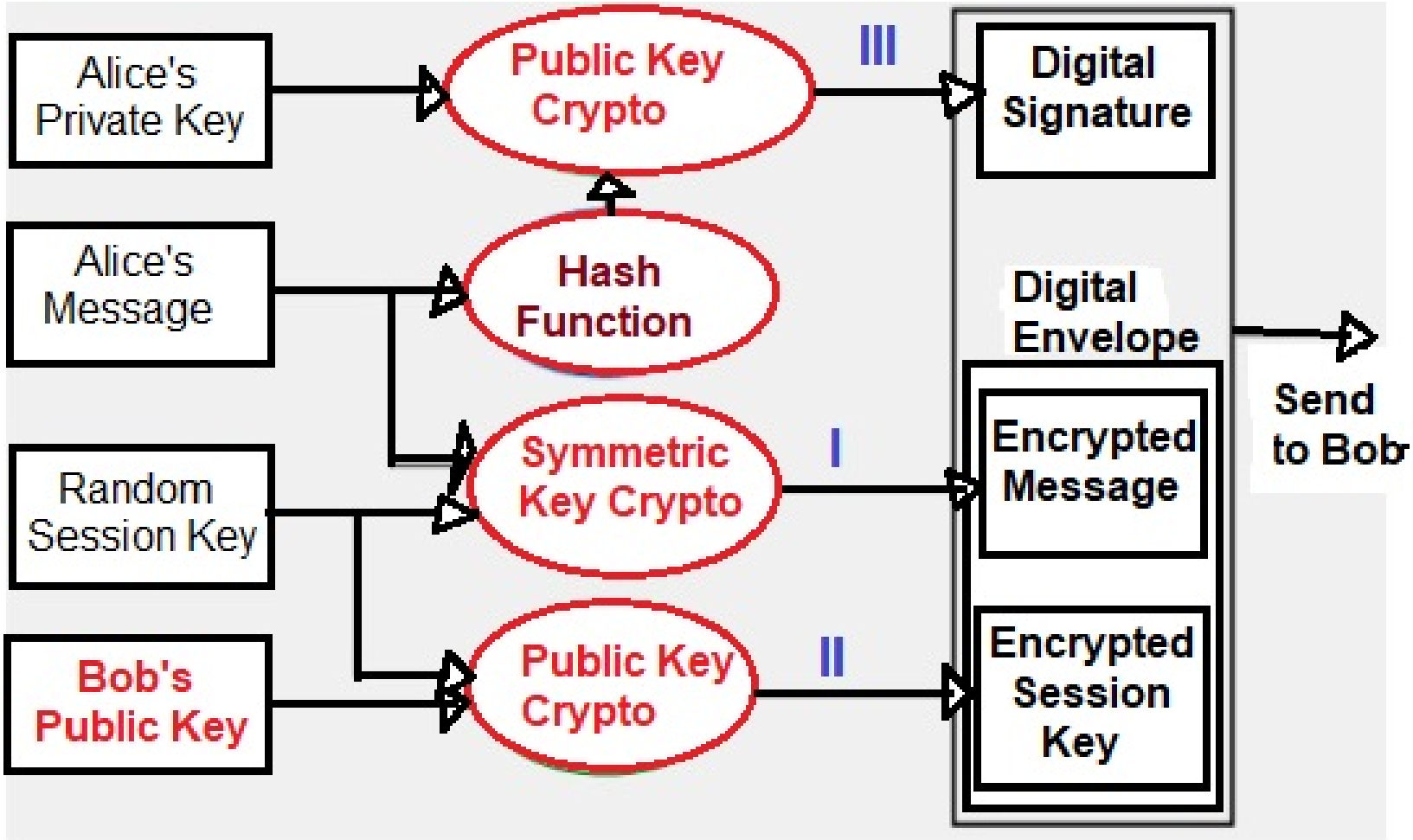
- **Confidentiality**
- **Integrity**
- **Authentication**

Goals and Mechanisms



- **Confidentiality**
- **Integrity**
- **Authentication**
- **Non-repudiation**

Goals and Mechanisms



- **Confidentiality**
- **Integrity**
- **Authentication**
- **Non-repudiation**

Security Notions

Unconditional security

- Given unlimited computational power, it is not possible to beak the cipher

Security Notions

Unconditional security

- Given unlimited computational power, it is not possible to beak the cipher

Computational security

- Given limited computing resources, breaking cipher is not possible
  (e.g., time needed for calculations is greater than age of universe)

Thank You