TE 582 - ADVANCED CRYPTOGRAPHY & NETWORK SECURITY

COURSE OBJECTIVES

- Deep theoretical grounding in classical and modern cryptography.
- Research exposure to quantum and post-quantum cryptography.
- Ability to critically analyze protocols using an information-theoretic approach.
- Develop research questions leading to publishable work.
- Understand how cryptographic primitives integrate into network security models.

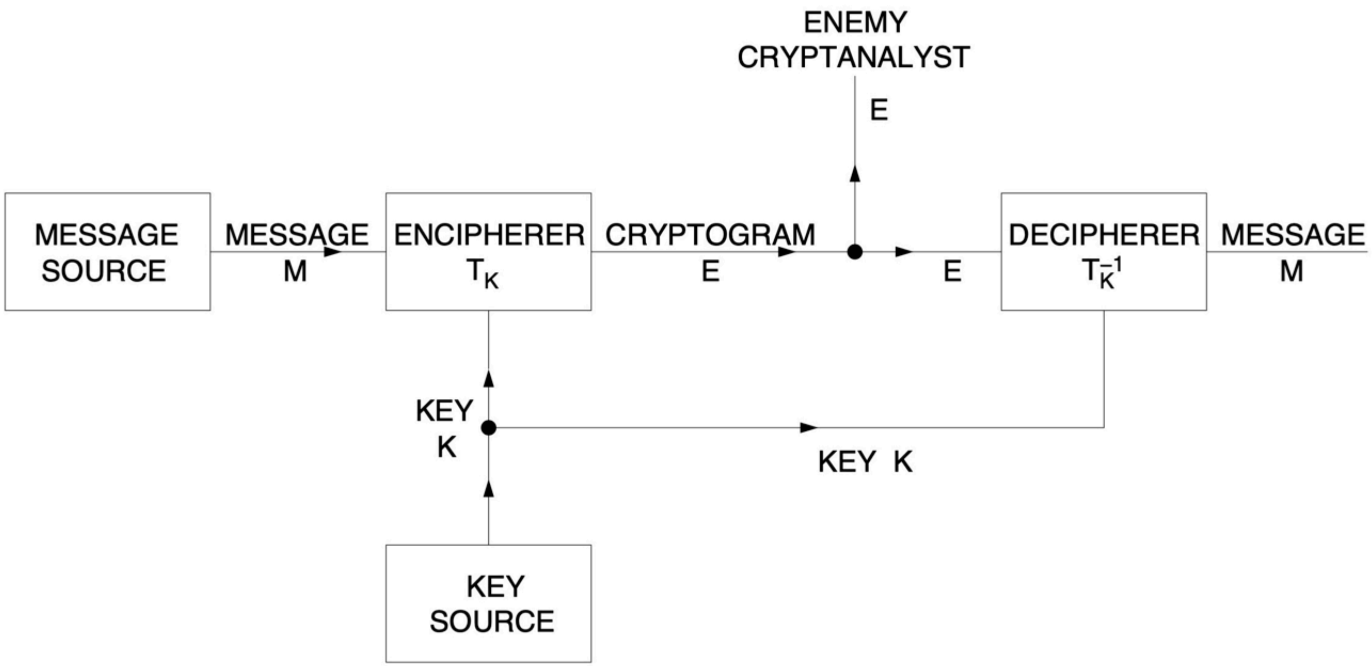
READING MATERIALS

- *Real-World Cryptography (2021)*, **David Wong**
- *Introduction to Modern Cryptography (2021)*, **Jonathan Katz, Yehuda Lindell**
- *Serious Cryptography: A Practical Introduction to Modern Encryption (2018)*, **Jean-Philippe Aumasson**
- *Hand of Applied Cryptography (2001)*, **Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone**

TYPES OF SECRECY SYSTEMS

- **Concealment systems:** hide the existence of the message.
- **Privacy systems:** require special equipment for recovery.
- **True secrey systems:** meaning is concealed by codes/ciphers; *(communication theory of secrecy systems)*

SECRECY SYSTEMS



$$E = f(M, K)$$

MATHEMATICAL MODEL

- A secrey system is a family of reversible transformations.

$$E_k : M \mapsto C$$

where M = message, C = cryptogram, K = key

- Each key and message has an a priori probability distribution.
- Cryptanalysis updates beliefs using a posteriori probabilities after interception.

REDUNDANCY OF LANGUAGE

- Natural languages contain statistical redundancy.
- Redundancy $\Rightarrow$ cryptanalysis is possible with limited ciphertext.

ALGEBRA OF SECREY SYSTEMS

- Two composition operations
  - **Product:** successive application of two systems.
  - **Weighted sum:** probablistic choice of two systems.
- These form a *linear associative algebra*.

PURE VS MIXED CIPHERS

- **Pure cipher:** set of transformations closed under composition; all keys equivalent (e.g., simple substitution).
- **Mixed cipher:** no such closure property.

THEORETICAL SECRECY

- **Perfect secrecy:** A posteriori probabilities = a priori probabilities, i.e.,

$$P(M|C) = P(M) \quad \forall \quad M, C$$

- **Condition:** numbe rof keys $\geq$ number of messages.
- **Example:** Vernam cipher (one-time pad).

EQUIVOCATION

- Measure of uncertainty about key/message after interception.
- Defined via conditional entropy:

$$H(K|C), \quad H(M|C)$$

- Decreases as ciphertex length increases.
- Defines *unicity distance*:

$$N_0 \approx \frac{H(K)}{R}$$

where $H(K)$ = key entropy, R = redundancy of message symbol.

PRACTICAL SECRECY

- Even when unique solution exists, labor to solve may vary.
- Trade-offs between; key size, error propagation, enciphering complexity, message expansion.

KEY INSIGHTS

- Security depends fundamentally on language redundancy and key size.
- Perfect secrecy requires as much key entropy as message entropy.
- Most practical systems are breakable after sufficient ciphertext is intercepted (unicity distance).
- Shannon's framework links cryptography with information theory (entropy, probability, equivocation).

THANK YOU