

Lecture 4

Requirements

- Two requirements for secure use of symmetric encryption:

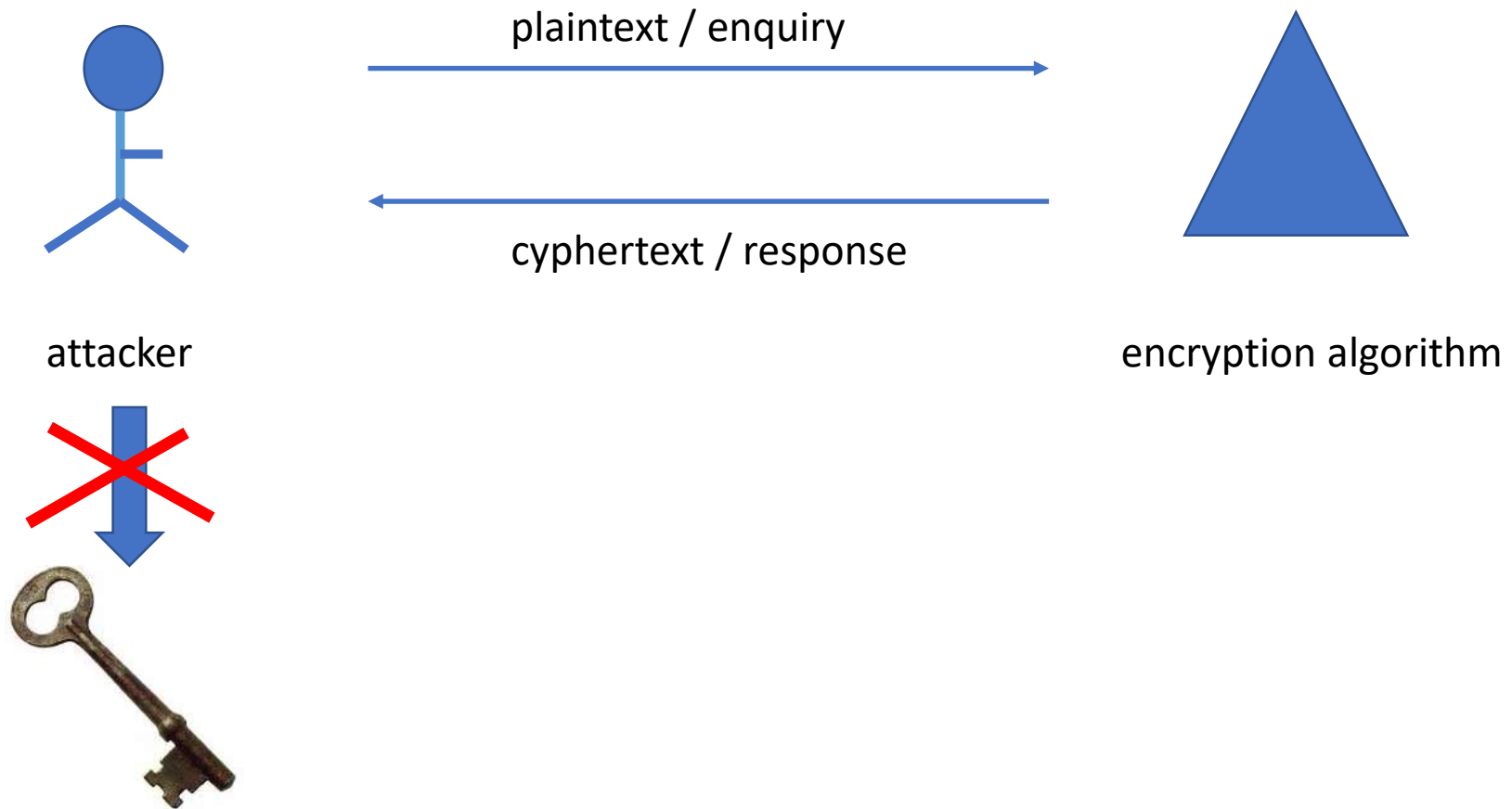
- a strong encryption algorithm
- a secret key known only to sender / receiver

$$Y = E_K(X)$$

$$X = D_K(Y)$$

- assume encryption algorithm is known
- the security of symmetric encryption depends on the secrecy of the key
- implies a secure channel to distribute key

A strong encryption algorithm



Secure Encryption Scheme

- **Unconditional security**

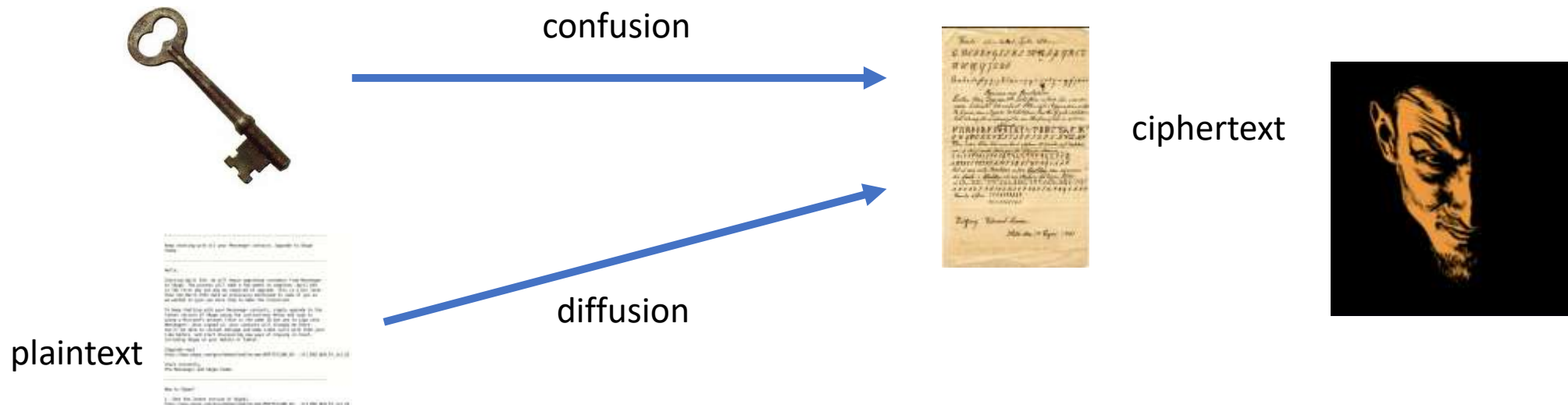
- no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext

- **Computational security**

- the cost of breaking the cipher exceeds the value of the encrypted information;
- or the time required to break the cipher exceeds the useful lifetime of the information

Desired characteristics

- Cipher needs to completely obscure statistical properties of original message
- more practically Shannon suggested combining elements to obtain:
 - Confusion – how does changing a bit of the key affect the ciphertext?
 - Diffusion – how does changing one bit of the plaintext affect the ciphertext?



Ways to achieve

- Symmetric Encryption:
 - substitution / transposition / hybrid
- Asymmetric Encryption:
 - Mathematical hardness - problems that are efficient to compute in one direction, but inefficient to reverse by the attacker
 - Examples: Modular arithmetic, factoring, discrete logarithm problem, Elliptic Logs over Elliptic Curves

Project

- TA Name: Lin, Yu
- Email: Yu.Lin@ttu.edu
- Form a group (no submission)
 - The project will be assigned as a group project. Six students will be considered a group for a project. Here is the link to enter your project group member names.
[FALL 2023 CS5342 PROJECT GROUP NAMES.xlsx](#)
 - It is recommended that one person in the group fills in the form to avoid multiple entries and submits project files on Blackboard. If you cannot get a group, contact the TA.
- Deadline to submit your group members is 11:59 PM on Sept 8th, 2023