CSC474/574 Homework 7

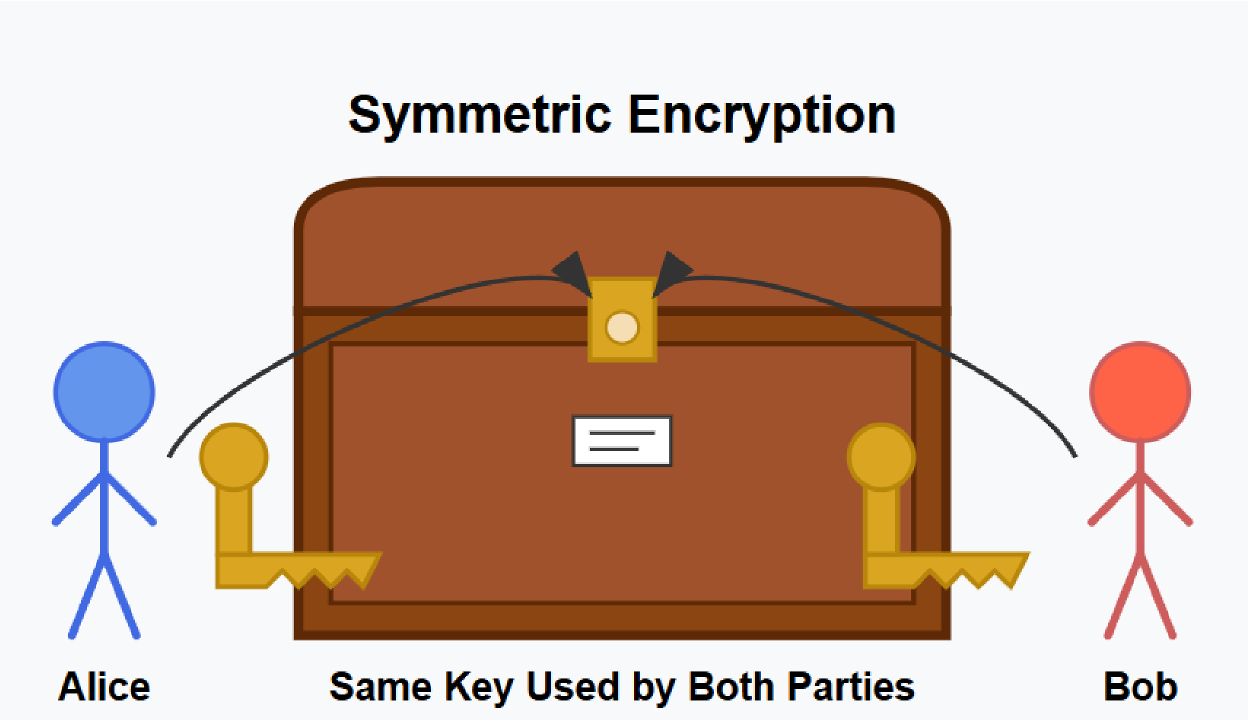
Junesh Gautam

April 29, 2025

Q1: Elaborate on what symmetric encryption is, what asymmetric encryption is, and what the difference is between these two.

Symmetric Encryption is like a **single-key treasure chest**:

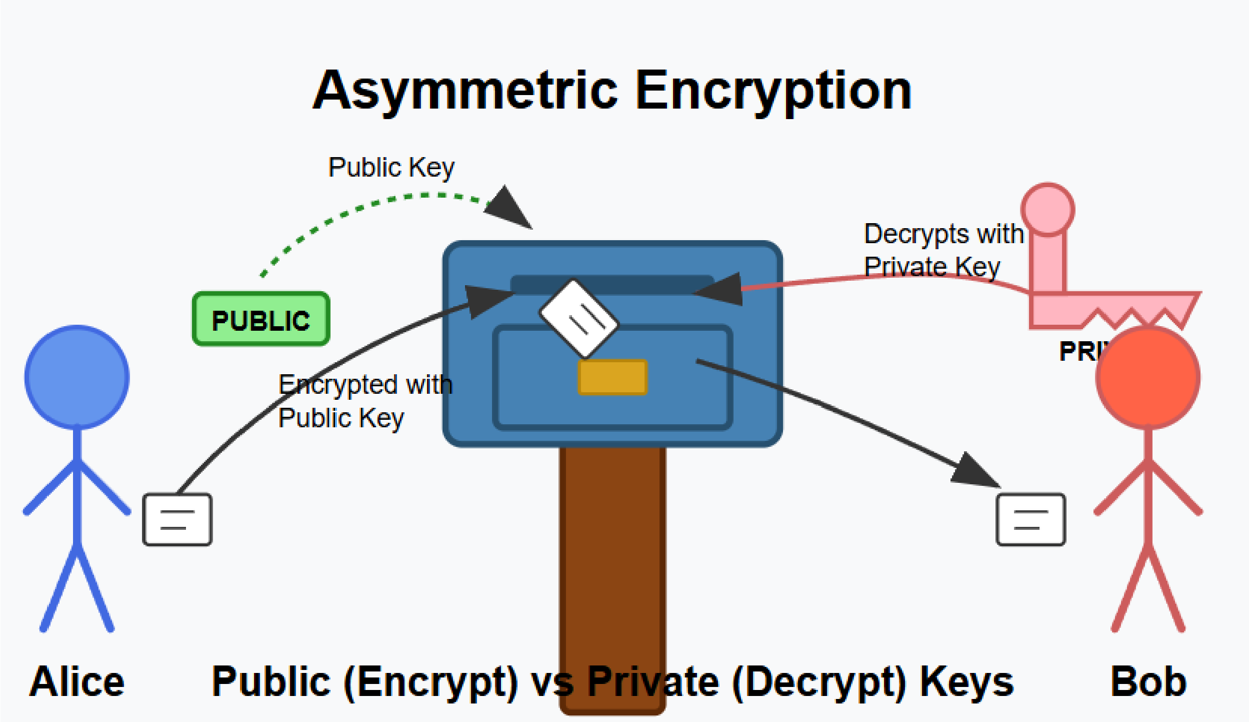
- Uses *one shared secret key* for both encryption and decryption
- Fast and efficient (e.g., AES, DES)
- **Analogy**: Imagine you and your friend share an actual key to lock/unlock a box of secret messages



Asymmetric Encryption is like a **public mailbox system**:

- Uses *two mathematically linked keys*: public key (shared) and private key (secret)
- Slower but enables secure key exchange (e.g., RSA, ECC)

- **Analogy**: Anyone can drop letters in your mailbox (public key), but only you have the key to open it (private key)


Asymmetric Encryption
Public Key
PUBLIC
Decrypts with Private Key
PRI
Encrypted with Public Key
Alice
Public (Encrypt) vs Private (Decrypt) Keys
Bob

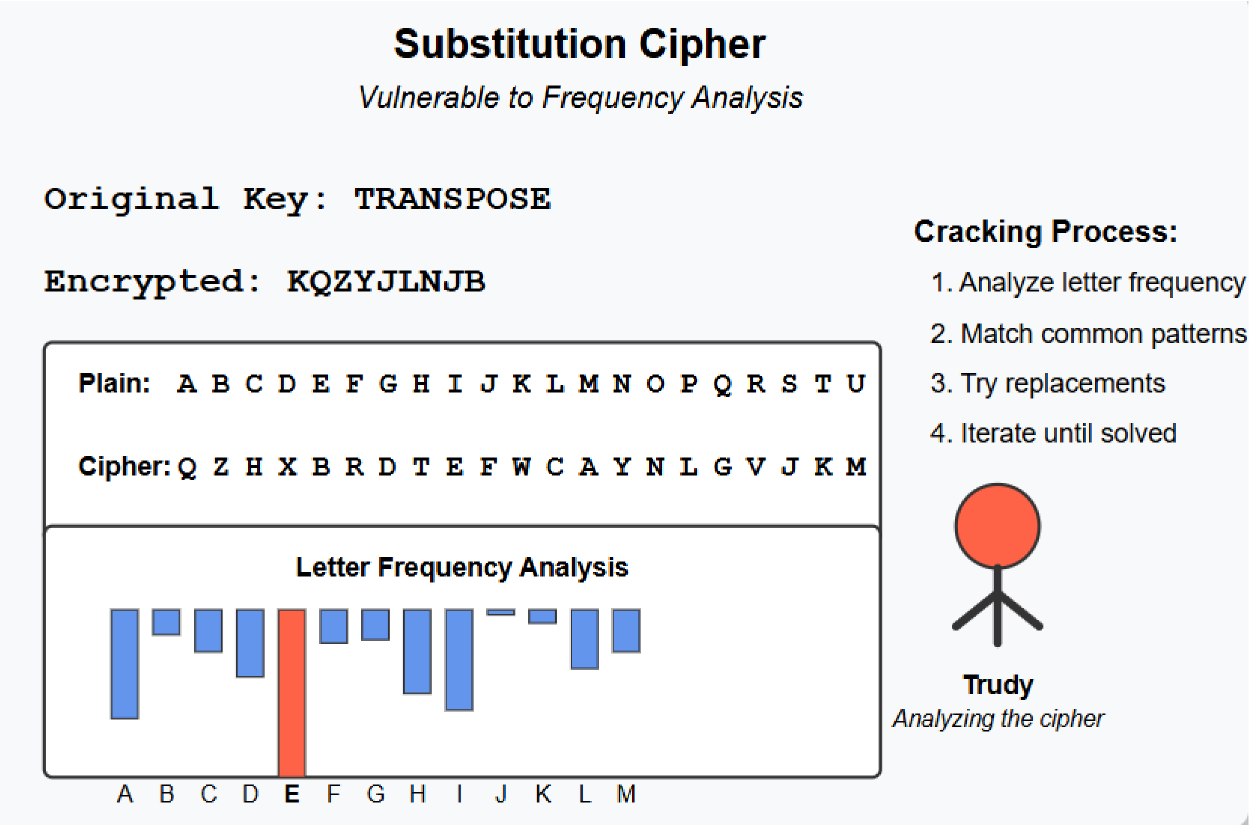
Key Differences:

	Symmetric	Asymmetric
Keys	1 shared key	2 linked keys
Speed	Fast	Slow
Use Case	Bulk encryption	Key exchange & signatures
Security	Key distribution risk	Quantum-vulnerable

Q2: Alice used a transposition cipher to encrypt her messages to Bob. For added security, she encrypted the transposition cipher key using a substitution cipher, and kept the encrypted cipher in her computer. Trudy managed to get hold of the encrypted transposition cipher key. Can Trudy decipher Alice's messages to Bob? Why or why not?

Yes, Trudy can decipher the messages through a *double decryption process*:

1. **Substitution Cipher Layer** (Key Encryption):
   - Substitution ciphers replace letters (A→X, B→Q, etc.)
   - Vulnerable to frequency analysis (e.g., E=13% in English)
   - **Analogy**: Like solving a "cryptogram" puzzle in newspapers



Substitution Cipher

Vulnerable to Frequency Analysis

Original Key: TRANSPOSE

Encrypted: KQZYJLNJB

Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
Cipher:	Q	Z	H	X	B	R	D	T	E	F	W	C	A	Y	N	L	G	V	J	K	M

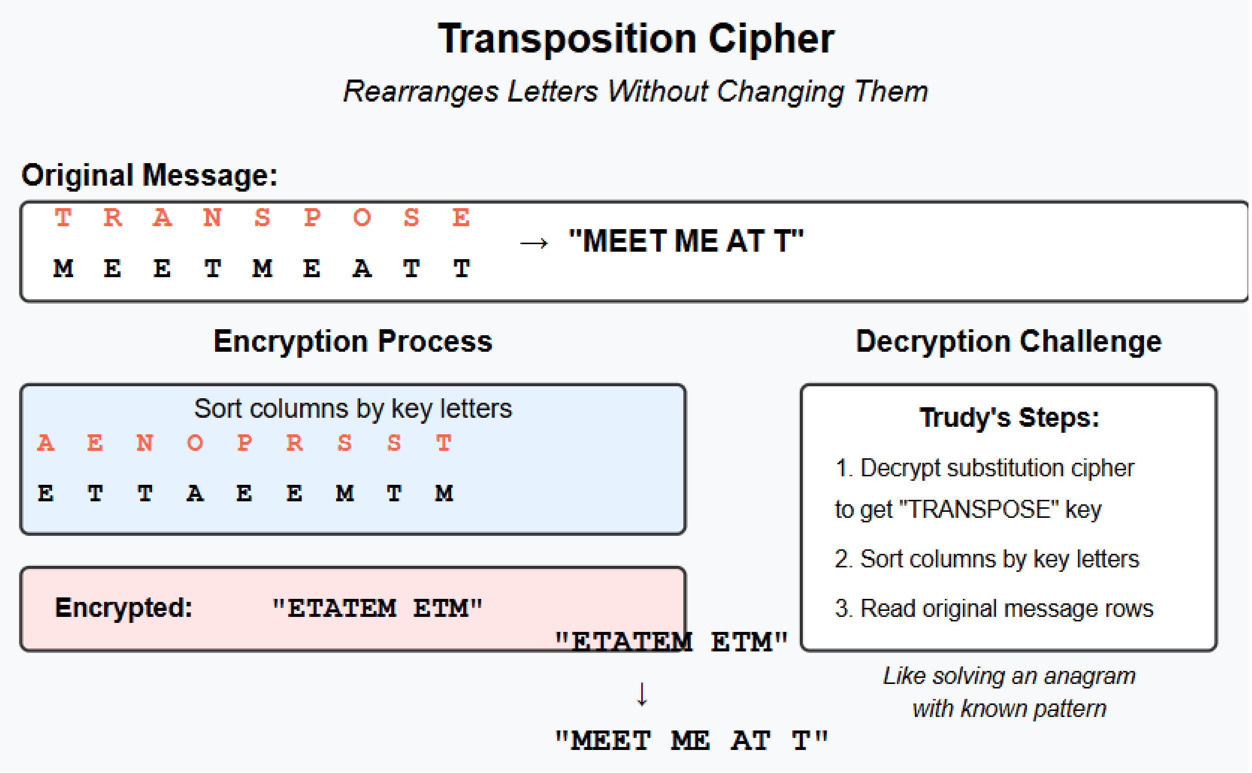
Cracking Process:

1. Analyze letter frequency
2. Match common patterns
3. Try replacements
4. Iterate until solved

Trudy

Analyzing the cipher

2. **Transposition Cipher Layer** (Message Encryption):
   - Rearranges letters (e.g., "HELLO" → "LOHLE")
   - Requires knowing the permutation pattern (key)
   - **Analogy**: Solving an anagram after knowing word length

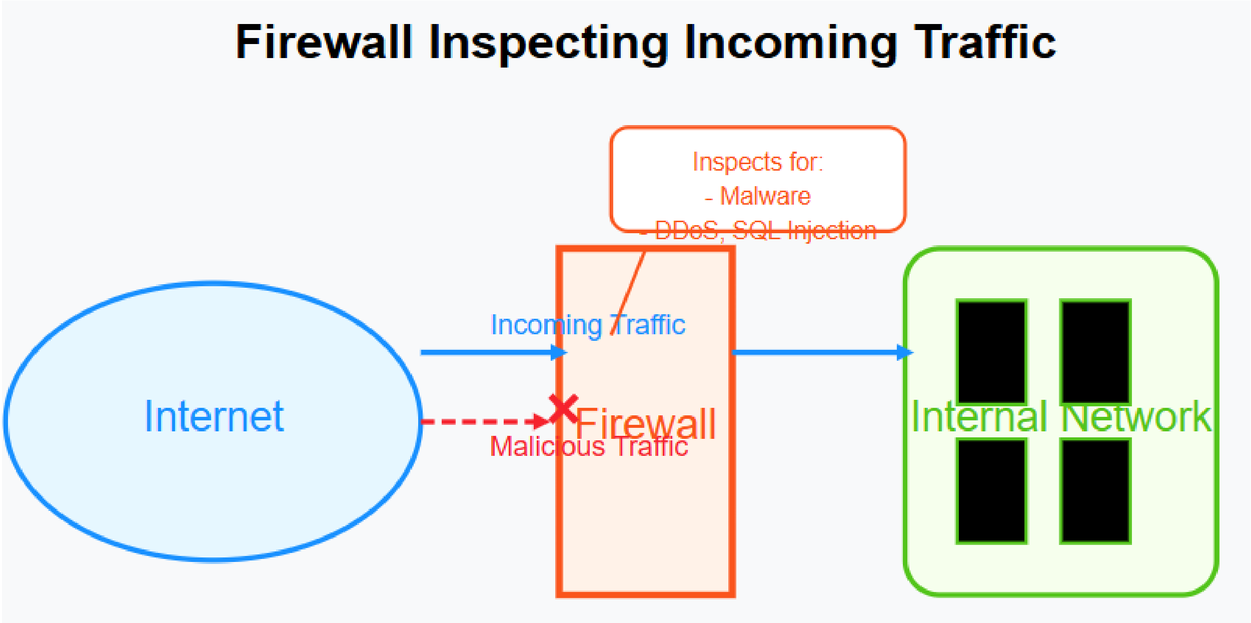


Why This Works: The substitution cipher adds *security through obscurity*, not real cryptographic strength. Once Trudy cracks the substitution layer (which is relatively easy), she gains the transposition key needed to decode the actual messages.

Q3: Give one reason why a firewall might be configured to inspect incoming traffic. Give one reason why it might be configured to inspect outgoing traffic. Do you think the inspections are likely to be successful? Any particular examples?

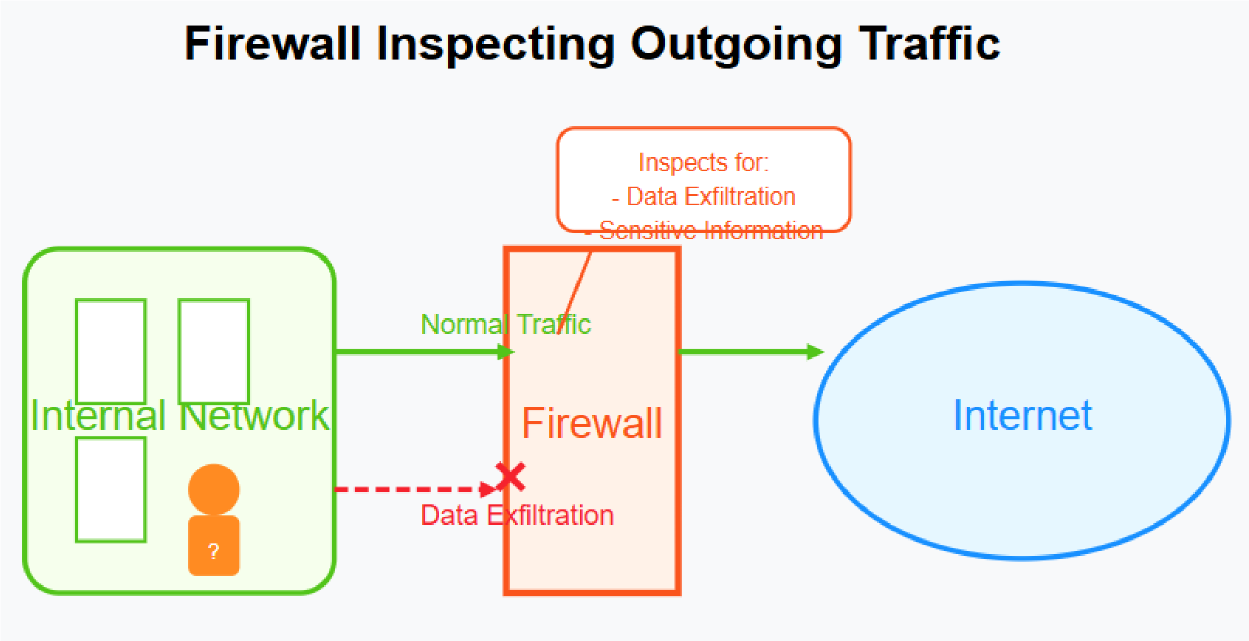
Incoming Traffic Inspection:

- **Purpose**: Block malicious actors (e.g., hackers, DDoS attacks)
- **Analogy**: Airport security checking luggage for prohibited items
- **Example**: Blocking SQL injection attempts in HTTP requests



Outgoing Traffic Inspection:

- **Purpose**: Prevent data exfiltration/internal threats
- **Analogy**: Factory checking outgoing shipments for stolen goods
- **Example**: Detecting employees emailing sensitive files



Success Factors:

- **Effective**: For known attack patterns (e.g., signature-based detection)

- **Ineffective**: Against zero-day exploits or encrypted traffic
- **Real Case**: 2017 Equifax breach - firewalls failed to detect encrypted exfiltration