Practical 1: Monoalphabetic Substitution

- **Primary weakness:**
  Monoalphabetic ciphers are weak against frequency analysis since letter patterns remain unchanged, making the cipher easy to break.
- **Decoding without key:**
  Use frequency analysis by comparing ciphertext letter frequencies with common English letters and refining guesses through context.
- **Encoding numbers/symbols:**
  It can include numbers and symbols if defined in the substitution table, but it still remains weak due to detectable patterns.
- **Substitution table:**
  It's a key mapping showing which plaintext letter replaces which ciphertext letter; encryption and decryption use this mapping.

Practical 2: Playfair Cipher

- **Primary weakness**
  Vulnerable to digraph (pair) frequency analysis because letter-pair patterns remain.
  Also weak to known-plaintext attacks and not secure for modern use.
- **How it differs from simple substitution**
  Encrypts letter **pairs** (digraphs) using a 5×5 key square instead of single letters.
  This hides single-letter frequencies, making simple frequency attacks harder.
- **What is a digraph**
  A digraph is a pair of letters encrypted together as one unit.
  If letters repeat or length is odd, insert a filler (commonly X) to form valid pairs.
- **Number of possible keys**
  Number of keys = **25! ≈ 1.5511×10^25**, which is about **2^83.7 ≈ 2^84** possible keys.
  (Your original wrote "283.7"; that was a typo — it should be ≈ 2^83.7.)

Practical 3: Vignere Cipher

- **Strengths & Weaknesses of Vignere**
  Strengths**:** Uses polyalphabetic substitution, making repeated letters encrypt differently.
  Weaknesses**:** Weak against frequency analysis if the keyword is short or reused.
- **Breaking Method of Vignere**
  Kasiski examination finds repeated patterns to estimate keyword length.
  Once known, ciphertext parts can be analyzed like Caesar ciphers to recover the key.
- **Significance of Key Length**
  Longer keys add more variation and improve security.
  If key = message length and random, it becomes an unbreakable one-time pad.
- **Comparison of Vignere with Other Ciphers**
  Vigenère repeats a keyword for shifts, while others (like Autokey) use non-repeating keys.
  It's simpler but weaker than more complex polyalphabetic ciphers.

Practical 4: Subsitution and Transposition Cipher

- **Basic Structure & Purpose**
  A product cipher combines substitution and transposition ciphers in sequence.
  This layering increases encryption complexity and makes cryptanalysis harder.
- **Components & Example**
  It uses substitution (replacing letters) and transposition (rearranging them).
  Example: “HELLO” → substitution → “KHOOR” → transposition → rearranged ciphertext.
- **Security Dependence**
  Security depends on the strength and secrecy of substitution and transposition keys.
  If either key is weak, the entire cipher becomes easy to break.
- **Ineffectiveness Scenarios**
  Less effective for high-security or large data due to weak keys and slow processing.
  Modern ciphers like AES are faster, stronger, and resist advanced attacks.

Practical 5: AES DES From Notes

Practical 6: RSA

- **Primary Use Cases**
  RSA is used for secure communication, digital signatures, and key exchange.
  It is widely applied in secure emails (PGP, S/MIME) and web encryption (HTTPS).
- **Key Steps**
  Generate keys using large primes (p, q) and compute n = p×q, ϕ(n), e, and d.
  Encrypt: C = M^e mod n; Decrypt: M = C^d mod n.
- **Modulus (n) Significance**
  n = p×q; it’s part of both public and private keys.
  RSA’s security depends on the difficulty of factoring n into p and q.
- **Real-World Example**
  Used in HTTPS to securely exchange session keys during the SSL/TLS handshake.
  RSA ensures authentication and protects data using public-private key encryption.

Practical 8: Wireshark

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what’s happening inside a network cable. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Applications of Wireshark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol internals

- **Promiscuous Mode:**
  Network interface captures **all packets** on the network, not just those addressed to it.
  Used in packet sniffing or network monitoring tools like Wireshark.
- **Non-Promiscuous Mode:**
  The interface captures **only packets meant for its own MAC address.**
  Used in normal network operation for regular communication.
- **Port Filter:**
  Captures packets based on **specific port numbers** (e.g., port 80 for HTTP).
  Used to monitor or block traffic on certain application ports.
- **Address Filter:**
  Filters packets using **source or destination IP/MAC addresses.**
  Helps capture traffic to/from specific devices.
- **Protocol Filter:**
  Captures packets of a **specific protocol** (e.g., TCP, UDP, ICMP).
  Useful to analyze certain types of network communication.
- **String Filter:**
  Searches for or captures packets containing a **specific text/string pattern** in data.
  Used for identifying keywords or content in network payloads.

Practical 9: nmap

Nmap is a network scanning tool used to discover hosts, open ports, and services on a network. It helps in network auditing, security assessment, and vulnerability detection.

- nmap -p 1-200 — Scan TCP ports 1–200 on the target to see which are open.
- nmap -p 80 — Check whether TCP port 80 (HTTP) is open on the target.
- nmap -F — Fast scan of Nmap's most common ports for a quick look.
- nmap -p- — Sweep all 65,535 TCP ports on the target (full TCP port scan).
- nmap -sT — TCP connect() scan (works without raw sockets; noisier, but usable unprivileged).
- nmap -sU — Scan UDP ports to detect UDP-based services.
- nmap -A — Aggressive scan: OS detection, version detection, NSE scripts, and traceroute.
- nmap -O — Attempt OS fingerprinting to guess the host's operating system.
- nmap 192.168.1.0/24 — Scan an entire subnet (CIDR) to discover live hosts and their open ports.