# Network & Information Security - Practical Answers

## 1. Perform Backup and Restore of the system.

To backup: Use `rsync -a /source /backup` on Linux or Windows Backup Tool.

To restore: Copy data back to the original directory.

## 2. Set up passwords to operating system and applications.

For OS: Use `passwd` in Linux or Control Panel in Windows.

For applications: Use settings or user management options to set strong passwords.

## 3. Apply security to file folder or application using access permissions and verify.

Linux: `chmod 700 filename`, `chown user:user filename`.

Windows: Right-click -> Properties -> Security tab.

## 4. Write a program to implement Caesar Cipher

```python
text = 'HELLO'
shift = 3
def caesar_encrypt(text, shift):
    return ''.join(chr((ord(c)-65+shift)%26+65) for c in text.upper())
print(caesar_encrypt(text, shift))
```

## 5. Write a program to implement Vernam Cipher

```python
message = 'HELLO'
key = 'XMCKL'
cipher = ''.join(chr(ord(m)^ord(k)) for m, k in zip(message, key))
```

## 6. Create and verify Hash Code for given message

```python
import hashlib
msg = 'Hello world'
hash_object = hashlib.sha256(msg.encode())
print(hash_object.hexdigest())
```

## 7. Write a program to implement Rail fence technique

```python
def rail_fence_encrypt(text, key):
    rail = ['']*key
    dir_down, row = False, 0
    for ch in text:
        rail[row] += ch
        if row == 0 or row == key-1: dir_down = not dir_down
        row += 1 if dir_down else -1
    return ''.join(rail)
```

## 8. Write a program to implement Simple Columnar Transposition technique

```python
def columnar_encrypt(msg, key):
    col = [''] * key
    for i, ch in enumerate(msg):
        col[i % key] += ch
    return ''.join(col)
```

## 9. Create and verify digital signature using tool (e.g. Cryptool)

Steps:

1. Open Cryptool -> Digital Signature.

2. Enter message.

3. Generate hash -> Encrypt hash with private key.

4. Verify with public key.

## 10. Use Steganography to encode and decode the message using any tool.

Use tools like `steghide`, `OpenStego`:

Encode: `steghide embed -cf image.jpg -ef message.txt`

Decode: `steghide extract -sf image.jpg`

## 11. Create and verify Digital Certificate using tool (e.g. Cryptool)

Use Cryptool:

1. Open -> Certificate Generation.

2. Fill details -> Export certificate.

3. Verify using public key.

## 12. Trace the origin of Email using any tool(e.g. email TrackerPro)

Steps:

1. Open email -> Show original headers.

2. Use Email Tracker Pro -> Paste headers.

3. Identify sender IP and location.

## 13. Trace the path of web site using Tracert Utility

`tracert www.example.com` (Windows) or `traceroute www.example.com` (Linux/Mac)

Shows the route from your system to the destination server.