solving DLP. However, DH is ~~not~~ vulnerable to man-in-the-middle attacks without authentication.

If the prime modulus is too small, DLP becomes feasible via algorithms like Pohlig-Hellman or Number Field Sieve, allowing an attacker to recover private keys & break the protocol.

Answer to the Q.No: 8

Let H & K be subgroups of G. Their intersections is nonempty (it contain the identity). For any $a, b \in H \cap K$, both H & K contain a & b, so ab^{-1} is in both H & K, hence in $H \cap K$. By the subgroup test, $H \cap K$ is a subgroup of G.

In $\mathbb{Z}$ under addition, $2\mathbb{Z}$ & $3\mathbb{Z}$ are subgroups. Their intersection $6\mathbb{Z}$ is also a subgroup.

Answer to the Q.NO: 6

The scaler matrics $S = \{aI : a \in \mathbb{R}^{\times}\}$ from a normal subgroup of $GL(2, \mathbb{R})$ because for any $A \in GL(2, \mathbb{R})$ & $aI \in S$, we have $A(aI)A^{-1} = aI$.

The factor group $GL(2, \mathbb{R})/S$ is the projective linear group $PGL(2, \mathbb{R})$ which corresponds to the group of projective transformations on the real projective line RP^1. Each coset represents a matrix up to non-zero scalar multiples, capturing the geometry of linear fractional transformations.

Answer to the Q.NO: 7.

Diffie-Hellman allows two parties to establish a shared secret over an insecure channel by exchanging public values derived from private random numbers & public parameters. The shared secret is computed as $g^{\wedge}(ab) \bmod p$ from private keys $*a*$ & $*b*$.

Security relies on the hardness of the Discrete Logarithim Problem - an eavsdropper cannot compute the shared secret from public values without

Answer to the Question NO: 4

The action $\sigma \cdot (i, j) = \{\sigma(i), \sigma(j)\}$ is well defined because permutations are bijections, so distinct elements map to distinct elements, & the set notations ensure order inpendence.

The orbit of $\{1,2\}$ is the entire set of 2-elements subsets of $\{1,2,3,4\}$ which has size 6. By the orbit-stablizer theorem, the stabilizer has size 4, consisting of permutation that either fix or swap 1 & 2 while freely permuting 3 & 4.

Answer to the Q. NO: 5

(i) The nonzero elements of $GF(2^2)$ form a group under multiplication because the field structure ensures assiociativity, identity (1) & inverses.

(ii) Yes, the set of nonzero elements is cyclic. The multiplicative group has order 3, which is prime, so it is cyclic.

Answer to the Question NO: 3

Traditional Ciphers (Caesar, Vigenere, Playfair)
key length: very short
Speed: very fast / Manual
Security: Extremely weak - broken by frequency analy-sis

Modern Symmetric Ciphers: (AES, DES)
Key length: DES (56 bit, now weak), AES (128-256 bit)
Speed: Optimized for hardware/software, AES particul-arly efficient
Security: Resists differential / linear cryptanalysis, brute-force protection, extensive cryptanalysis testing.

Answer to the Q.NO: 2

```
import time
import os

class SimplePRNG:
    def __init__(self, low, high):
        self.low = low
        self.high = high
        self.state = int(time.time_ns()) ^ os.getpid()

    def next(self):
        self.state = (self.state * 1103515245 + 12345) &
                                                0x7FFFFFFF
        return (self.state % (self.high - self.low + 1)) +
                                                self.low

prng = SimplePRNG(1, 100)
print = SimplePRNG(1, 100)
print(prng.next())
```

The algorithm combines:

1. Timestamp
2. Process ID
3. Modulus operation.

Answer of Question NO: 1

Quantam computing breaks RSA & Ecc via Shor's algorithm, underomining most digital security. To replace them, post-quantam algorithms rely on mathematical problems believe to be ~~slo~~ solved hard even for quantam computers:

1. Lattice-based - Rely on the learning error problems
2. Hash-based - Security depends on hash function collision resistance
3. Code-based — Based on the hardness of decoding random linear codes.

These resistance quantam cryptanalysis because Shor's algorithm doesn't apply to their underlying problems, the best known quantam attacks offer only minor speedups, not the exponential breakdown seen for RSA/Ecc.

Answer to the Q. NO: 9

$\mathbb{Z}_n$ is commutative because multiplication modulo n inherits commutativity from integer multiplication.

$\mathbb{Z}_n$ has zero divisors if n is composite. For example in $\mathbb{Z}_6$, $2 \cdot 3 \equiv 0 \pmod 6$.

$\mathbb{Z}_n$ is a field iff n is prime, as every nonzero element then has a multiplicative inverse modulo n.

Answer to the Q. NO: 10 :

multiplicative inverse modulo n.

Answer to the Q. No: 10 :

DES is vulnerable due to its 56 bit effective key length, which is too short for modern brute-force attacks. It's 64 bit block is also small increasing collision risks in large ~~area~~ data.

Modern cryptanalysis like differential and linear attacks further when DES & its Feistel structure & S-Boxes - secure in the 1970 are now outdated. 3DES offers temporary relief but is slow & being phased out.

AES replaced DES with 128/192/256 bit keys, stronger resistance to attacks & higher efficiency, making DES obsolete for sequre applications.