Diffie–Hellman: Theory, Requirements, and CTF Challenge Design

August 13, 2025

1 Why "p Must Be Prime for the Multiplicative Group mod p to be Cyclic"

1.1 Multiplicative Group mod p

- Definition: The set $\{1, 2, 3, \ldots, p-1\}$ with multiplication modulo p as the operation.
- Excludes 0 because it has no multiplicative inverse.
- Example for $p = 7$:
  - Set: $\{1, 2, 3, 4, 5, 6\}$
  - $3 \times 5 \equiv 1 \pmod 7$ since $15 = 2 \times 7 + 1$.

1.2 Group Properties

A group $(G, \cdot)$ satisfies:

1. **Closure:** $a, b \in G \Rightarrow a \cdot b \in G$.
2. **Identity:** $1 \in G$ such that $a \cdot 1 = a$.
3. **Inverses:** $\forall a \in G, \exists a^{-1}$ with $a \cdot a^{-1} = 1$.
4. **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

1.3 Cyclic Groups

A group is *cyclic* if there exists a generator g such that:

$$\{g^1 \bmod p, g^2 \bmod p, \ldots, g^{p-1} \bmod p\} = \{1, 2, \ldots, p-1\}.$$

Example ($p = 7$, $g = 3$):

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod 7.$$

1.4 Why Prime p Matters

- If p is prime, $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$ is always cyclic.
- Guarantees at least one generator g producing all elements.
- If p is composite, $\mathbb{Z}_n^*$ may not be cyclic.

1.5 Counterexample (Non-prime p)

Let $p = 8$, coprime set: $\{1, 3, 5, 7\}$.

- $g = 3$: $3^1 \equiv 3$, $3^2 \equiv 1$ — misses 5 and 7.
- $g = 5$: $5^1 \equiv 5$, $5^2 \equiv 1$ — misses 3 and 7.

1.6 Plain English Summary

We want a generator g whose powers cover all nonzero residues mod p before repeating. Prime p ensures this is possible; composite p may break it.

2 Diffie–Hellman Variable Requirements

p **(Prime Modulus)**
: Large prime, often a *safe prime* $p = 2q + 1$ to prevent small subgroup attacks.

g **(Generator)**
: Integer $2 \leq g \leq p - 2$, generating a large subgroup.

a, b **(Private Keys)**
: Random integers in $[2, p - 2]$, kept secret.

A, B **(Public Keys)**

$$A = g^a \bmod p, \quad B = g^b \bmod p$$

S **(Shared Secret)**

$$S = B^a \bmod p = A^b \bmod p$$

3 Why Diffie–Hellman is Hard to Break

- Based on the hardness of the *Discrete Logarithm Problem* (DLP).
- No efficient classical algorithm for large p.
- Quantum computers with Shor's algorithm could solve DLP efficiently — motivating post-quantum cryptography.