

Experiment 4 — Diffie-Hellman Key Exchange

Name: Atharva Tamhankar

UID: 2022300127

Experiment: Exp04

Aim.

Implement Diffie-Hellman (DH) to allow two parties to agree on a shared secret over an insecure channel.

Role of p and g .

- p is a large prime modulus; security depends on the difficulty of discrete logarithm modulo p .
- g is a generator of a large prime-order subgroup modulo p ; using safe primes ($p = 2q + 1$) and a generator of order q mitigates this risk.

Private exponents.

- Each party chooses a private exponent (a, b) uniformly at random from $[2, p-2]$ using a cryptographic RNG (secrets).
- Never reuse private exponents.

Shared secret and KDF.

- Public values: $A = g^a \bmod p$, $B = g^b \bmod p$.
- Shared secret: $K = g^{ab} \bmod p$. Apply a KDF (SHA-256) to derive a symmetric key; do not use K directly.

Implementation choices.

- Language: Python 3. Uses `pow(base, exp, mod)` and Miller–Rabin for prime generation (demo).
- Parameters: demo primes (64/128/512/1024 bits) for lab; production should use 2048+ bit MODP or ECDH.
- Demo encryption: XOR stream with derived key (FOR DEMO ONLY — NOT SECURE).

Security considerations & attacks.

- Discrete Log Hardness: use sufficiently large primes in production (≥ 2048 bits).
- MITM: DH without authentication is vulnerable to active MITM; use certificates or authenticated key exchange (TLS).
- Small-subgroup attacks: use safe primes and verify public values are in correct subgroup.
- RNG & side-channels: use cryptographic RNG and constant-time operations where applicable.

Sample Input–Output.

Run 1 (64-bit prime, plaintext = "hello world"):

- p (bits=64), $g=2$ selected.
- Generated keys: $A=18773199211485791838$, $B=11005874175577578102$
- Shared secret: $K_A = K_B$ (62 bits).
- Derived key (SHA-256): 9fd5e46d...
- Ciphertext: 37065b2a9dc83fa144f8a9
- Recovered: hello world

Run 2 (128-bit prime, plaintext = "Diffie Hellman works!"):

- p (bits=128), $g=2$ selected.
- Generated keys: $A=237225672899342855128160994091939944647$
 $B=234984620865063202412510929027530540258$
- Shared secret: $K_A = K_B$ (127 bits).
- Derived key (SHA-256): 5bcf5f9b...

- Ciphertext: 1e2a2c462abb17f4fa8173f47c1f0f93e5cb8bceea
- Recovered: Diffie Hellman works!