CSE 484 In-section Worksheet #5

Q1. Using modular exponentiation and without evaluating the exponent directly, what is 3^5 mod 11?

$3^5 \bmod 11 = ((3 \bmod 11)\ (3^5 \bmod 11)) \bmod 11)$

$= ((3 \bmod 11)\ (((3^2 \bmod 11)\ (3^2 \bmod 11)) \bmod 11) \bmod 11)$

$= (3\ (9 * 9 \bmod 11)) \bmod 11 = 3 * 4 \bmod 11 = 1$

Q2. In one Diffie-Hellman exchange, which variables are public? What does Alice know? Bob? (some options: p, g, x, y) What do they send to each other? What is the shared key?

Public: p, g

Private: x, y

Alice sends $g^x \bmod p$

Bob sends $g^y \bmod p$

Key = $g^{xy} \bmod p = (g^x \bmod p)^y \bmod p$

Q3. What does Z_p^* represent? What is the mathematical definition of co-primality for p and q?

Z_p^* is the set of values relatively prime to p

Co-primality means gcd(p, 1) = 1

Q4. Let p = 11. Let g = 5. Alice's private key is x=4. Bob's private key is y=8. What is their shared key?

Key = $g^{xy} \bmod p = 5^{4*8} \bmod 11 = 3$

Q5. What does Euler's Totient function compute for some integer p? What is ϕ(35)?

It computes the number of integers in Z_p^*

$\phi(35) = \phi(7 * 5) = \phi(7)\ \phi(5) = 6 * 5 = 24$

Q6. What is the public key in RSA? The private key? (some options: p, q, n, e, d)

Public: (e, n)

Private: (d, n)

Q7. In a RSA communication, Alice is trying to send a message with value 16 to Bob. Her public key is (5,35) and his private key is (5,35). What is the resulting cipher text? How do we decrypt this?

$C = M^e \bmod n = 16^5 \bmod 35 = 11$

$M = C^d \bmod n = (M^e)^d \bmod n = 11^5 \bmod 11 = 16$

Q8. Given that Alice generates the (large) prime numbers p=5 and q=7. What do we choose for e? What are its bounds? What is a value for d that works? Why not 3?

e cannot be 3 (3 is not invertible modulo 24), next smallest prime = 5

$d = e^{-1} \bmod n \rightarrow d * e = 1 \bmod n$

For small values brute force, generally use extended Euclidean algorithm

Here d = 5 works

Q9. Are RSA or Diffie-Hellman sufficient for all of our security needs? Which cryptography goals do they meet?

No!

RSA

- Output is deterministic, does not provide integrity
- Provides authenticity, privacy

Diffie-Helman

- Provides privacy