CSE 484 In-section Worksheet #5

MAC & Hashing

Q1. What security goal are we able to achieve by the use of MAC?
Integrity- A recipient can recompute the MAC for a message and check it matches the MAC attached to the message.
Authenticity- Only someone who knows the key can compute the correct MAC for a given message.

Q2. After submitting your lab1 md5 hashes, you decide to modify the solution without the TAs knowing. Which known cryptographic vulnerability of md5 can you take advantage of?
Collision resistance- MD5 is not collision resistant and is possible (but hard) to create another submission that maps to the same MD5 hash.

Number Theory

Q3. Using modular exponentiation and without evaluating the exponent directly, what is 3^5 mod 11?

$$3^5 mod\ 11 = \big((3\ mod\ 11)(3^4 mod\ 11)\big)\ mod\ 11$$
$$= \Big((3\ mod\ 11)\big((3^2\ mod\ 11)(3^2\ mod\ 11)\big)\ mod\ 11\Big)\ mod\ 11$$
$$= \Big(3 * \big((9 * 9)\ mod\ 11\big)\Big) mod\ 11 = (3 * 4)\ mod\ 11 = 1$$

Q4. Produce the generating sequence for g = 4 and p = 7. What order is it?
Run $4^x\ mod\ 7$ for x in {1, 2, 3, 4, 5...} until you find a repeating pattern.
$4^1\ mod\ 7 = 4$, $4^2\ mod\ 7 = 2$, $4^3\ mod\ 7 = 1$, etc.
The repeating pattern ends up being {4, 2, 1, 4, 2, 1, ...}, so the order (# unique values) is 3.

Generally, we use g as a primitive root (every relatively prime number of p is congruent to a power of g mod p) to p so the raised powers modded by p distribute about p evenly, making longer sequences.
For further reading on the use of generators in Diffie Hellman (and about the computational and decisional Diffie-Hellman assumptions), this is a good read:
https://florianjw.de/en/insecure_generators.html.

Diffie-Hellman

Q5. 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? What makes it secure?

Public: p, g. Private: Alice knows X, Bob knows Y.

Alice sends g^x mod p, Bob sends g^y mod p.

Key = g^{xy} mod p

DH is secure thanks to a few assumptions:

- Discrete log problem: Given g^x mod p, it is hard to compute x. If p is a prime modulus hundreds of digits long, it is computationally infeasible to find a matching x for a given g^x mod p. See Khan Academy's video on the discrete log problem: https://youtu.be/SL7J8hPKEWY [1 min 55 sec]
- Computational Diffie Hellman problem: Given a generator g, g^x, and g^y, it's hard to compute g^{xy}. Much easier to compute when you know x or y, but you'd have to compute x or y from taking the discrete log (which is hard).
- Decisional Diffie Hellman problem: It's hard to tell whether you have g^{xy}, or a random value.

Q6. 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?

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

RSA

Q7. What does Euler's Totient function compute for some integer p? What is ϕ(35)?

Euler's Totient computes the number of integers relatively prime to p.

$\phi(35) = \phi(7 * 5) = \ \phi(7) * \phi(5) = 6 * 4 = 24$

Q8. 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?

Alice sends $C = M^e \ mod \ n = 16^5 \ mod \ 35 = 11.$

Bob decrypts this using $M = C^d \ mod \ n = (M^e \ mod \ 11)^d \ mod \ n = 11^5 \ mod \ 11 = 16.$

Q9. 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?

From above, $\phi(35) = 24$.

In this case, e can't be 3 (since 3 is not relatively prime to $\phi(35) = 24$), next smallest prime is 5.

Recall $ed \equiv 1 \ mod \ \phi(n)$, so $d = e^{-1} mod \ \phi(n) = 5^{-1} mod \ 24 = 5 \rightarrow d = 5$ works.

For small values, we can brute force by using the extended Euclidean algorithm, but for larger numbers, can use Wolfram Alpha.

Security Goals Review

Q10. What are the 4 security goals that we are trying to achieve?

Confidentiality
Integrity
Authentication
Authenticity

Q11. Are RSA or Diffie-Hellman sufficient for all of our security needs? Which security goals do they meet?

No!

RSA has deterministic output, and doesn't provide integrity by itself. But, it does provide authenticity and privacy.

Diffie Hellman provides privacy.