2018 fall, Internet Security, mid-term 3:35 – 4:30pm

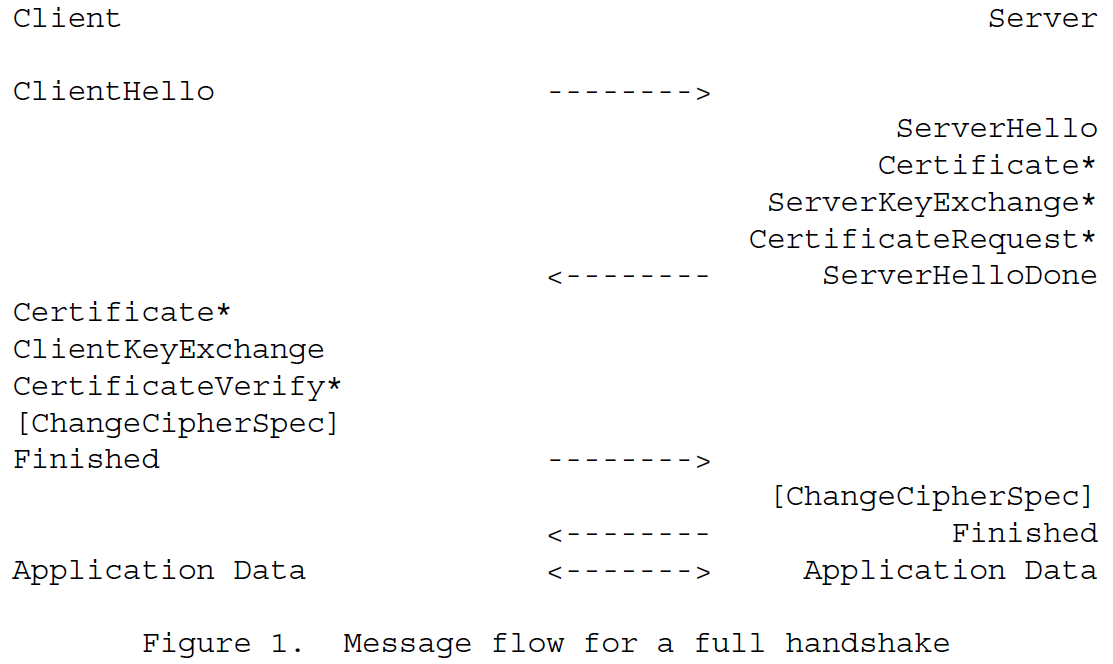
1. AES consists of 4 modules: SubBytes, ShiftRows, MixColumns, and AddRoundKey. Classify these modules into three primitives in symmetric cryptography: substitution cipher, permutation cipher, and exclusive-or.

Sub, per, sub, x-or

2. The message flow for handshake protocol in TLS 1.1/1.2 is shown below. Assume the RSA cipher is used to send a pre\_master secret. Explain which message includes which input parameter of PRF(•) below. Explain how pre\_master\_secret is encrypted and decrypted. The formula to generate the master secret is given by:

master\_secret = PRF(pre\_master\_secret, "master secret", ClientHello.random + ServerHello.random);

ClientHello.random in clienthello



ServerHello.random in serverhello

Pre\_master\_Secret in clientkeyexchange

Certificate shows the public key of the server.

Client encrypts the pms by the public key of the server

Then the server decrypts the pms by its private key.

3. Let us make an RSA encryption when the modulus n=pq (55=5\*11) and the message m is 8. The public key e is 7 and the private key d is 23. Explain the relation between e and d. Show how the ciphertext is calculated by the sender and how it is decrypted by the receiver. Use that 220 mod 55 = 1. Which of the values (n, p, q, m, e, d) are known to the attacker?

C = 8^7 mod 55 = 2^21 mod 55 = 2

m = C^d mod 55= 2^23 mod 55 = 8 mod 55 = 8

attacker 는 n, e, C 를 안다

4. An ElGamal signature is generated by Alice where the message is m (to be received by Bob) and the modulus p is a prime number. She chooses a private key 1 < x < p-1, computes her public key: y = ax mod p, chooses a random secret k s.t. 1  k  (p-1) and gcd(k,p-1)=1, computes a temporary key: r = ak mod p, computes k-1, and computes s = k-1 (m-xr) mod (p-1). What is sent from Alice to Bob? Bob verifies the signature by checking whether V1 equals V2, where V1 is am mod p. What is V2?

Y = a^x mod p

choose k

r = a^k mod p, k^-1, s = k^-1(m-xr) mod p-1

alice 가 보내느 것은? (a,y,p ,r,s,m)

bob은 어떻게 확인하는가?

V1 = a^m mod p = a^(m – xr + xr) = a^k\*1/k(m-xr + xr) =

v2 = r^s a^xr = r^x y^r mod p

5. OCSP stapling solves some problems in OCSP. What are they?

Client’s privacy, client overhead to contact the OCSP server, OCSP server availability

클라이언트의 privacy, 클라이언트의 OCSP 서버와 contact 해야 하는 overhead, OCSP server의 availability