2021 spring, Internet Security, mid-term 2-3pm

1. security 서비스 중에 authentication과 non-repudiation이 무엇인지 각각 한 문장으로 설명하고, 둘 다 제공하는 보안 메커니즘이 무엇인지 쓰시오. (15 points)

authentication : 송신자가 누구인지 확인할 수 있고 위조불가능

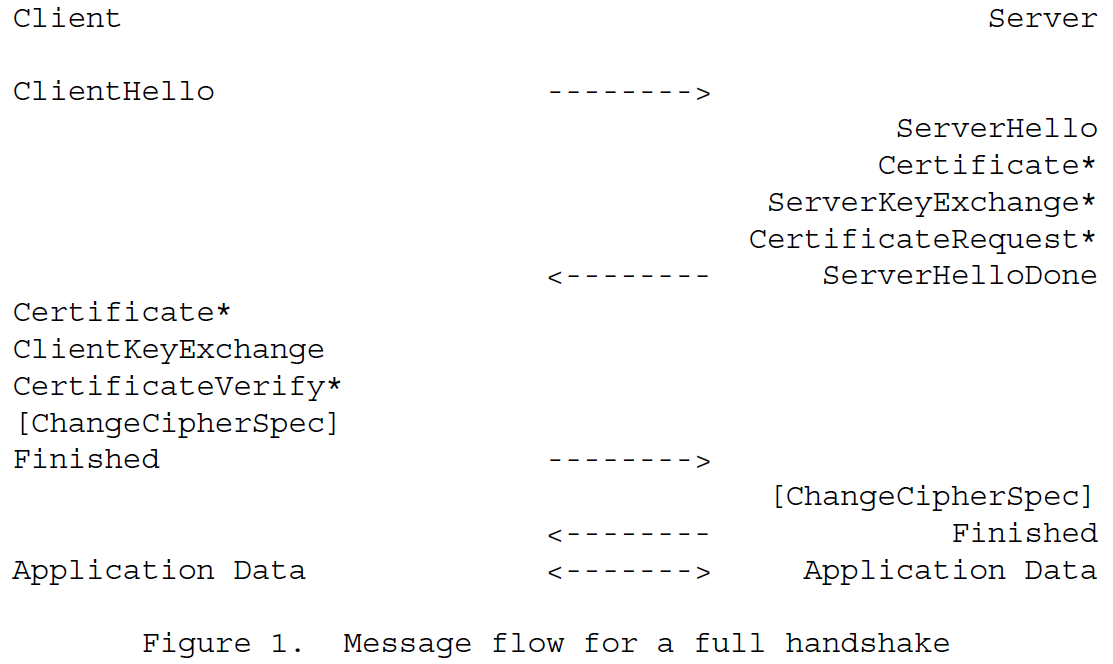
non-repudiation : 송신자가 자신이 보냈음을 부정할 수 없음

디지털 서명

2. AES는 4가지 모듈이 있다. SubBytes, ShiftRows, MixColumns, and AddRoundKey. 각각의 모듈이 substitution cipher, permutation cipher, and exclusive-or 중 어느 것으로 분류되는지 쓰시오. (15p)

sub per sub xor

3. TLS 1.1/1.2의 메세지 흐름이 아래에 있다. 서버의 RSA 인증서를 사용하여 client가 pre\_master\_Secret을 보낸다고 했을때 왜 forward secrecy를 보장할 수 없는가? TLS 1.3에서는 어떻게 forward secrecy를 보장하는가? (30p)



서버의 RSA 인증서를 사용하면, 암호화/복호화에 server의 public key, private key를 사용하게 되는데, 이 경우에 나중에 traffic을 server의 private key로 열어볼 수 있다.

Hello 와 동시에 random 넘버를 주고 받고, 이를 이요왜 DHE\_RSA를 사용하고 이 때 사용한 g^cs mod p 는 세션이 종료됨과 동시에 서버에서 삭제한다.

4. RSA 알고리즘에서 공개키 modulus n=pq (7\*19)으로 주어지고, 메세지는 6이다. 공개키의 지수 e는 5이고 비밀키(private key) d는 65이다. 이러한 인자들 중에 공격자가 아는 값들은 무엇인가? 또한 어떻게 암호화되고 복호화 되는지 계산하시오. 다음의 계산식들을 이용해도 좋다. (20p)

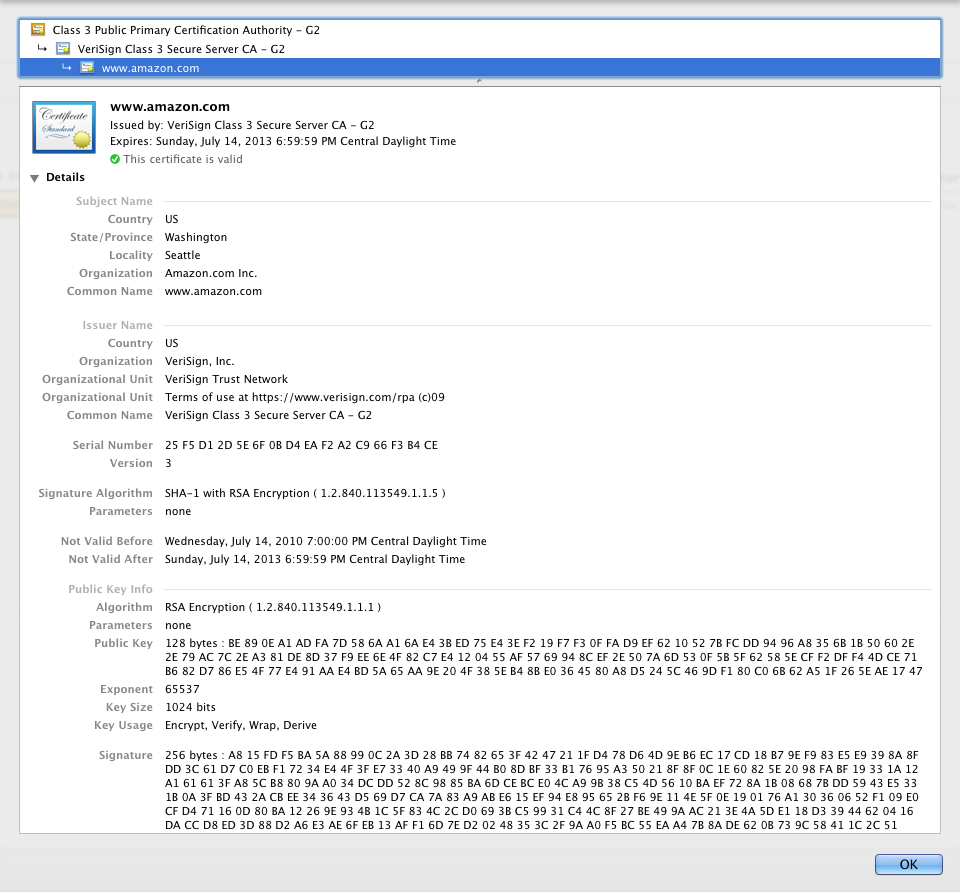
64 mod 133 = 99, 622 mod 133 = 120, 12032 mod 133 = 43

공격자가 아는 값은 ciphertext 6^5 mod 133, n = 133, 공개키 e = 5 이다.

암호화 : 6^5 mod 133 = 62

복호화 62 ^ 65 mod 133 = 62 ^ (64 + 1) mod 133 = 62 ^ 64 \* 62 mod 133 = 120^32 \* 62 mod 133 = 43 \* 62 mod 133 = 6

5. 다음은 인증서의 일부를 발췌하였다. 여기서 public key(RSA의 modulus)의 길이(1024 bits)와 signature의 길이(2048 bits)가 다른 이유는 무엇인가? Signature도 RSA를 사용하여 만들었다고 가정한다. (20p)



Signature 는 CA의 서명으로, CA 가 자신의 private key를 이용해 암호화해놓은 값이다.

따라서 이 값은 CA의 public key 길이와 같기 때문에, subject의 public key와는 길이가 다를 수 있다.