Homework 10

Question 1

4.1. Samantha uses the RSA signature scheme with primes $p = 541$ and $q = 1223$ and public verification exponent $e = 159853$.

(a) What is Samantha's public modulus? What is her private signing key?

(b) Samantha signs the digital document $D = 630579$. What is the signature?

Question 2

4.2. Samantha uses the RSA signature scheme with public modulus $N = 1562501$ and public verification exponent $e = 87953$. Adam claims that Samantha has signed each of the documents

$$D = 119812, \quad D' = 161153, \quad D'' = 586036,$$

and that the associated signatures are

$$S = 876453, \quad S' = 870099, \quad S'' = 602754.$$

Which of these are valid signatures?

Question 3

4.3. Samantha uses the RSA signature scheme with public modulus and public verification exponent

$$N = 27212325191 \quad \text{and} \quad e = 22824469379.$$

Use whatever method you want to factor N, and then forge Samantha's signature on the document $D = 12910258780$.

Question 4 : Elgamal Digital Signature Scheme

Public parameter creation	
A trusted party chooses and publishes a large prime p and primitive root g modulo p.	
Samantha	**Victor**
Key creation	
Choose secret signing key $1 \leq a \leq p-1$. Compute $A = g^a \pmod{p}$. Publish the verification key A.	
Signing	
Choose document $D \bmod p$. Choose random element $1 < k < p$ satisfying $\gcd(k, p-1) = 1$. Compute signature $S_1 \equiv g^k \pmod{p}$ and $S_2 \equiv (D - aS_1)k^{-1} \pmod{p-1}$.	
Verification	
	Compute $A^{S_1} S_1^{S_2} \bmod p$. Verify that it is equal to $g^D \bmod p$.

(A) Explain why verification works.

(B) Explain why if Eve can solve discrete logarithm problem, then Eve can forge Samantha's signature?

Question 5

4.8. Suppose that Samantha is using the Elgamal signature scheme and that she is careless and uses the same random element k to sign two documents D and D'.

(a) Explain how Eve can tell at a glance whether Samantha has made this mistake.

(b) If the signature on D is (S_1, S_2) and the signature on D' is (S_1', S_2'), explain how Eve can recover a, Samantha's private signing key.

(c) Apply your method from (b) to the following example and recover Samantha's signing key a, where Samantha is using the prime $p = 348149$, base $g = 113459$, and verification key $A = 185149$.

$$D = 153405, \qquad S_1 = 208913, \qquad S_2 = 209176,$$
$$D' = 127561, \qquad S_1' = 208913, \qquad S_2' = 217800.$$