MATH/CMSC 456 (Washington) Exam 2 Spring 2017

You may use calculators.

1. (15 points = 10+5) Alice and Bob are trying to implement triple encryption with DES. Let E_K denote DES encryption with key K and let D_K denote decryption.
(a) Alice chooses two keys, K_1 and K_2, and encrypts using the formula $c = E_{K_1}(D_{K_2}(E_{K_1}(m)))$.
Bob chooses two keys, K_1 and K_2, and encrypts using the formula $c = E_{K_1}(E_{K_2}(E_{K_2}(m)))$.
One of these methods is more secure than the other. Say which one is weaker and explicitly give the steps that can be used to attack the weaker system. You may assume that you know ten plaintext-ciphertext pairs.
(b) What is the advantage of using D_{K_2} instead of E_{K_2} in Alice's version?
2. (10 points) Let p be a 500-digit prime and let g be a primitive root mod p. Define a hash function by $H(x) = g^x \pmod{p}$. Although H can be computed quickly, it is not fast enough to be a good hash function. State one more property of cryptographic hash functions that H does not satisfy and one property that H satisfies. You must justify your answers.
3. (10 points) You use a random number generator to generate 10^9 random 15-digit numbers. What is the probability that two of the numbers are equal? Your answer should be accurate enough that you can say whether it is likely or unlikely that two of the numbers are equal.
4. (15 points) You set up a $(2, 30)$ Shamir threshold scheme, working mod the prime 73 (so there are 30 people and any 2 can determine the secret). Two of the shares are $(1, 13)$ and $(3, 12)$. A third share is $(4, *)$, where the part denoted by * is unreadable. What is the correct value of * ?
5. (20 points = 10 + 5 + 5) Suppose p is a large prime and g is a primitive root mod p. Suppose $g^s \equiv h \pmod{p}$, where s is secret. Everyone knows g, h, p. Peggy want to use a zero-knowledge proof to convince Victor that she knows s. They do the following protocol:
1. Peggy chooses a random r_1 and lets $r_2 = s - r_1$.
2. Peggy computes $h_1 \equiv g^{r_1}$ and $h_2 \equiv g^{r_2} \pmod{p}$ and sends h_1 and h_2 to Victor.
3. Victor randomly chooses $i = 1$ or $i = 2$ and asks Peggy for r_i, which Peggy sends.
4. Victor checks that $h_i \equiv g^{r_i} \pmod{p}$.
5. They repeat several times.
(a) Suppose Peggy does not know s. Explain how she can still succeed in every round of this protocol.
(b) What step needs to be added in order to make it very unlikely that Peggy can succeed in every repetition when she does not know s?
(c) Suppose Peggy knows s but is lazy and uses the same r_1 and r_2 in two different repetitions. How can Victor recognize that this is happening, and what can he do to find the secret s?
6. (15 points = 5+10) Recall the RSA signature scheme: Alice chooses distinct large primes p and q, computes $n = pq$, and chooses e and d with $de \equiv 1 \pmod{(p-1)(q-1)}$. She signs m by computing $s \equiv m^d \pmod{n}$. The signed message is (m, s). A signature (m, s) is valid if $s^e \equiv m \pmod{n}$.
(a) Suppose Eve knows that (m, s) is a valid signed message. How can she find a signature for m^7? (Recall that Eve cannot use d as part of the signing process, because she does not know d.)
(b) If Eve wants to find a message m such that $(m, 123)$ is a valid signed message, she computes $m \equiv 123^e \pmod{n}$. Suppose that Alice signs the hash $H(m)$ instead of signing m, where H is a publicly known hash function. Give the formulas that are used for signing a message m and verifying that (m, s) is a valid signed message, and explain why Eve should be unable to produce a valid signed message $(m, 123)$.
7. (15 points = 5+10) On the elliptic curve $E: \quad y^2 \equiv x^3 + x \pmod{7}$, compute
(a) $\infty + (1, 3)$
(b) $(1, 3) + (5, 2)$