MATH/CMSC 456 (Washington) Exam 2 May 3, 2005

1. (20 points = 10+10) A, B, C participate in a Shamir $(3,2)$ secret sharing scheme. They work mod 11. A receives the share $(1,5)$, B receives $(2,9)$, and C receives $(3,3)$.
(a) Show that at least one of the three shares is incorrect.
(b) Suppose A and C have correct shares. Find the secret.

2. (30 pts = 10+10+10) (a) Let K be the DES key consisting of all 1's. Explain why DES encryption E_K is the same as DES decryption D_K (that is, $E_K(x) = D_K(x)$ for all x).
(b) Suppose H is a cryptographic hash function. Nelson designs a new hash function H_1 as follows: Let x be an input. Nelson computes $H(x)$, then lets K be the rightmost 56 bits of $H(x)$. He then computes the DES encryption $E_K(00000\cdots 0)$, where $00000\cdots 0$ is the message consisting of 64 0's. The resulting 64-bit output is what Nelson calls $H_1(x)$. State what attack Eve can use to find a collision for H_1, and why the attack should work (on present-day computers).
(c) Let $H(x)$ be a cryptographic hash function. Nelson tries again. He takes a large prime p and a primitive root α for p. For an input x, he computes $\beta \equiv \alpha^x \pmod{p}$, then sets $H_2(x) = H(\beta)$. The function H_2 is not fast enough to be a hash function. Find one other property of hash functions that fails for H_2, and explain why it fails.

3. (15 points = 10+5) Recall the ElGamal signature scheme: Alice wants to sign a message m. She chooses a prime p, a primitive root α, and a secret integer a, and computes $\beta \equiv \alpha^a \pmod{p}$. The numbers p, α, β are made public. To sign m, Alice computes integers r and s. The signed message is (m, r, s). Bob verifies the signature by checking that $\beta^r r^s \equiv \alpha^m \pmod{p}$.
(a) Suppose Eve chooses $r_1 \equiv \alpha^{-1}\beta \pmod{p}$ and $s_1 \equiv -r_1 \pmod{p-1}$. This allows Eve to forge a message m_1. Determine what the message m_1 is.
(b) Explain how to use a hash function to prevent the forgery in part (a). What property of a hash function is used here?

4. (15 points) Suppose n is the product of two large primes, and that s is given. Peggy wants to prove to Victor, using a zero knowledge protocol, that she knows a value of x with $x^2 \equiv s \pmod{n}$. Peggy and Victor do the following:
(1) Peggy chooses three random integers r_1, r_2, r_3 with $r_1 r_2 r_3 \equiv x \pmod{n}$.
(2) Peggy computes $x_i \equiv r_i^2$, for $i = 1, 2, 3$ and sends x_1, x_2, x_3 to Victor.
(3) Victor checks that $x_1 x_2 x_3 \equiv s \pmod{n}$.
Design the remaining steps of this protocol so that Victor is convinced that the probability is less than a 1% that Peggy is lying.

5. (20 points = 10+10) (a) Let p be a large prime. Alice chooses a secret integer k and encrypts messages by the function $E_k(m) = m^k \pmod{p}$. Suppose Eve knows a cipher text c and knows the prime p. She captures Alice's encryption machine and decides to try to find m by a birthday attack. She makes two lists. The first list contains $c \cdot E_k(x)^{-1} \pmod{p}$ for some random choices of x. Describe how to generate the second list, state approximately how long the two lists should be, and describe how Eve finds m if her attack is successful.
(b) (this part has no relation to part (a)) The number 12347 is prime. Suppose Eve discovers that $2^{10000} \cdot 79 \equiv 2^{5431} \pmod{12347}$. Find an integer k with $0 < k < 12347$ such that $2^k \equiv 79 \pmod{12347}$.