

1. (a) It is very easy to find collisions. For example,  $h(m + 2^{128}) = h(m)$ . Also, it is easy to find preimages: if  $0 < y < 2^{128}$ , then  $h(y) = y$ .  
 (b) Eve will not succeed. She will obtain each 20-bit message exactly once. There will be no way to determine which is the correct plaintext and corresponding key.  
 (c) The key for each round is extracted from these 64 bits, so the key for each round consists of all 1's. Decryption is accomplished by using these keys in reverse order. Since they are all the same, reverse order is the same as non-reverse order. Therefore, encryption is the same as decryption, so  $E_K(E_K(m)) = m$ .

2. Let  $p$  and  $q$  be two distinct, large primes, and let  $n = pq$ .

- (a)  $\gcd(x - 2, n)$  is a nontrivial factor of  $n$ , therefore  $p$  or  $q$ .  
 (b) Alice uses the Chinese Remainder Theorem to find  $x$  satisfying  $x \equiv 2 \pmod{p}$  and  $x \equiv -2 \pmod{q}$ . Then  $x^2 \equiv 4 \pmod{p}$  and  $x^2 \equiv 4 \pmod{q}$ , hence  $x^2 \equiv 4 \pmod{n}$ , but  $x \not\equiv \pm 2 \pmod{n}$ .

3. (a)  $de = 1 + (p - 1)(q - 1)k$  for some integer  $k$ . Therefore,

$$c^d \equiv x^{de} \equiv x \cdot (x^{(p-1)(q-1)})^k \equiv x \cdot 1^k \pmod{n}$$

by Euler's Theorem. Therefore,  $c^d \equiv x$ .

- (b) Since  $m^3 \equiv 1 \pmod{n}$ , the ciphertext is  $c \equiv m^7 \equiv m \cdot (m^3)^2 \equiv m \cdot 1^2 \equiv m \pmod{n}$ . Therefore, the ciphertext is the plaintext, so Eve can read it without any decryption.

4. (a) Victor checks that  $X_1 + X_2 = B$ . Then he chooses  $i = 1$  or  $2$  at random and asks Peggy to send  $r_i$ . Victor then checks that  $X_i = r_i A$ . They repeat the procedure, starting with (i), at least 10 times (since  $2^{-10} < .001$ ).

(b) (i) Peggy chooses random  $r_1$  and lets  $r_2 = k - r_1$ . (ii) Peggy computes  $x_1 \equiv \alpha^{r_1}$  and  $x_2 \equiv \alpha^{r_2} \pmod{p}$ . (iii) Peggy sends  $x_1, x_2$  to Victor.

5. (a) We have  $v_1 \equiv \beta^r r^{-rv^{-1}} \equiv \beta^r (\beta^v \alpha^u)^{-rv^{-1}} \equiv \alpha^{ar - arv^{-1} - urv^{-1}} \equiv \alpha^{-urv^{-1}}$ , and  $v_2 \equiv \alpha^m \equiv \alpha^{su} \equiv \alpha^{-ruv^{-1}}$ . Therefore  $v_1 \equiv v_2$ , so the signature is valid.

(b) In part (a), we choose the message by letting  $m \equiv su \pmod{p-1}$ . Therefore once  $u, v$  are chosen, it is unlikely that  $\alpha^{h(m)} \equiv \alpha^m \pmod{p-1}$ . So the signature will probably not be valid.

6. (a) We have the matrix equation

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

This yields  $c_0 = 1, c_1 = 0, c_2 = 0$ .

(b) The line through  $(1, 2)$  and  $(6, 3)$  is  $y \equiv \frac{1}{5}(x - 1) + 2 \equiv 3x + 6 \pmod{7}$ . Intersect with the curve:  $(3x + 6)^2 \equiv x^3 + 3$ . The sum of the roots is the negative of the coefficient of  $x^2$ ,

so  $9 \equiv 1 + 6 + x$ , which yields  $x = 2$ . The third point of intersection has  $y = 3x + 6 \equiv 5 \pmod{7}$ . Reflect across the  $x$ -axis to get  $(2, 2)$ .

(c) The slope of the line through the two points is  $1/5 \pmod{35}$ . When she tries to evaluate  $1/5 \pmod{35}$ , she finds  $\gcd(5, 35) = 5$ , so she obtains a factor of 35. (This is what happens in the elliptic curve factorization method.)

**7.** (a) Since  $\alpha^{10^{18}} \equiv 1$ , the powers of  $\alpha$  repeat after  $10^{18}$  steps, so the answer to the discrete log can be taken to be less than  $10^{18}$ .

(b) Make two lists: First:  $\beta\alpha^{-i}$  for around  $10^9$  random choices of  $i$ . Second:  $\alpha^j$  for around  $10^9$  random choices of  $j$ . We expect a match:  $\beta\alpha^{-i} \equiv \alpha^j$ , which yields  $k = i + j$ .

(c) The first list contains the numbers  $\beta\alpha^{-10^9 i}$  for  $0 \leq i < 10^9$ . The second list contains  $\alpha^j$  for  $0 \leq j < 10^9$ . A match yields  $k = i + 10^9 j$ . Since every  $k$  with  $0 \leq k < 10^{18}$  can be written in this form, we always get a match.

(d) The attack in (c) is deterministic: it guarantees success (and it guarantees exactly one match). The attack in (b) is probabilistic: it has a good chance of success (and it might produce no matches, or it might produce several matches).

**8.** Let the decryption function be  $y = \alpha x + \beta \pmod{26}$ . We are given that  $3 \equiv \alpha \cdot 6 + \beta$  and that  $14 \equiv \alpha \cdot 1 + \beta$ . Subtracting yields  $11 \equiv -5\alpha \pmod{26}$ . This yields  $\alpha \equiv 3$ . Therefore,  $\beta \equiv 3 - 6 \cdot \alpha \equiv 11$ . The decryption function is  $y = 3x + 11 \pmod{26}$ . Therefore  $S = 18$  decrypts to  $13 = n$ , and  $P = 15$  decrypts to  $4 = e$ . The plaintext is *done*.