MATH/CMSC 456 (Washington) Exam 2 Solutions Spring 2017

1. (15 points = 10 + 5) **(a)** Bob's is weaker. Use a Meet-in.the-Middle attack. Choose a plaintext-ciphertext pair (m, c). Make two lists: (1) $E_K(E_K(m))$ for all keys K. (2) $D_L(c)$ for all keys L. Look for matches between the two lists. For each pair (K, L) that yields a match, test whether $E_L(E_K(E_K(m))) = c$ for the other nine plaintext-ciphertext pairs. Probably only one key pair survives. This yields the key.
(b) Backwards compatibility: If a 3-DES computer communicates with a 1-DES computer, it can let $K_1 = K_2$ and get single encryption.
2. (10 points) It is easy to find collisions: $H(x) = H(x+p-1)$ by Fermat's theorem. It is preimage resistant: Given y, it is hard to find x such that $g^x \equiv y \pmod p$ since this is a discrete log problem.
3. (10 points) There are $N = 10^{15}$ "birthdays" and $r = 10^9$ "people." The probability is approximately

$$1 - e^{-r^2/2N} = 1 - e^{-500} \approx 1.$$

Therefore, it is very likely that two of the numbers are equal.
4. (15 points) The line through $(1, 13)$ and $(3, 12)$ has slope $(12 - 13)/(3 - 1) = -1/2 \equiv 36 \pmod{73}$. The equation of the line is $y \equiv 36(x - 1) + 13$. When $x = 4$, we have $y \equiv 36(4 - 1) + 13 = 121 \equiv 48 \pmod{73}$. So $* = 48$.
5. (20 points = 10+5+5) (a) In each round, Peggy chooses random r_1 and r_2. They do not have to have any relation to s.
(b) Step 2.5: Victor checks that $h_1 h_2 \equiv h \pmod p$.
(c) Victor will see that h_1 and h_2 are the same as before. He asks for the r_j that he didn't ask for before and computes $s = r_1 + r_2$.
6. (15 points = 5+10) (a) Since $s^e \equiv m \pmod n$, we can raise each side to the 7th power and obtain $(s^7)^e \equiv m^7$. Therefore, (m^7, s^7) is a valid signed message.
(b) Alice computes $s \equiv H(m)^d \pmod n$. Then (m, s) is valid if $H(m) \equiv s^e \pmod n$. If $(m, 123)$ is valid, then $H(m) \equiv 123^e \pmod n$. It is hard to find m since H is preimage resistant.
7. (15 points = 5+10) (a) $\infty + (1, 3) = (1, 3)$.
(b) The line through $(1, 3)$ and $(5, 2)$ has slope $(2 - 3)/(5 - 1) = -1/4 \equiv 5 \pmod 7$. The line is $y \equiv 5(x - 1) + 3 = 5x - 2$. Intersect with $y^2 \equiv x^3 + x$ to get $0 \equiv x^3 - 25x^2 + \cdots$. Then $25 =$ sum of roots $= 1 + 5 + x$, so $x \equiv 5 \pmod 7$. The y-value is $5x - 2 = 23 \equiv 2$. Reflect across the x-axis to get the answer: $(5, 5)$.

MATH/CMSC 456 (Washington) Exam 2 Solutions Spring 2017

1. (10 points) It is easy to find collisions: $H(x) = H(x+p-1)$ by Fermat's theorem. It is preimage resistant: Given y, it is hard to find x such that $g^x \equiv y \pmod{p}$ since this is a discrete log problem.

2. (15 points) The line through $(1, 13)$ and $(3, 12)$ has slope $(12 - 13)/(3 - 1) = -1/2 \equiv 30 \pmod{61}$. The equation of the line is $y \equiv 30(x - 1) + 13$. When $x = 5$, we have $y \equiv 30(5 - 1) + 13 = 133 \equiv 11 \pmod{61}$. So $* = 11$.

3. (10 points) There are $N = 10^{16}$ "birthdays" and $r = 10^{10}$ "people." The probability is approximately

$$1 - e^{-r^2/2N} = 1 - e^{-5000} \approx 1.$$

Therefore, it is very likely that two of the numbers are equal.

4. (15 points = 5+10) (a) Since $s^e \equiv m \pmod{n}$, we can raise each side to the 5th power and obtain $(s^5)^e \equiv m^5$. Therefore, (m^5, s^5) is a valid signed message.

(b) Alice computes $s \equiv H(m)^d \pmod{n}$. Then (m, s) is valid if $H(m) \equiv s^e \pmod{n}$. If $(m, 765)$ is valid, then $H(m) \equiv 765^e \pmod{n}$. It is hard to find m since H is preimage resistant.

5. (20 points = 10+5+5) (a) In each round, Peggy chooses random r_1 and r_2. They do not have to have any relation to s.

(b) Step 2.5: Victor checks that $h_1 h_2 \equiv h \pmod{p}$.

(c) Victor will see that h_1 and h_2 are the same as before. He asks for the r_j that he didn't ask for before and computes $s = r_1 r_2$.

6. (15 points = 5+10) (a) $\infty + (1, 0) = (1, 0)$.

(b) The line through $(1, 0)$ and $(4, 4)$ has slope $(4-0)/(4-1) = 4/3 \equiv 5 \pmod{11}$. The line is $y \equiv 5(x-1) = 5x - 5$. Intersect with $y^2 \equiv x^3 + x$ to get $0 \equiv x^3 - 25x^2 + \cdots$. Then $25 =$ sum of roots $= 1 + 4 + x$, so $x \equiv 9 \pmod{11}$. The y-value is $5x - 5 = 40 \equiv 7$. Reflect across the x-axis to get the answer: $(9, 4)$ (or $(9, -7)$).

7. (15 points = 10 + 5) **(a)** Bob's is weaker. Use a Meet-in.the-Middle attack. Choose a plaintext-ciphertext pair (m, c). Make two lists: (1) $E_K(E_K(m))$ for all keys K. (2) $D_L(c)$ for all keys L. Look for matches between the two lists. For each pair (K, L) that yields a match, test whether $E_L(E_K(E_K(m))) = c$ for the other nine plaintext-ciphertext pairs. Probably only one key pair survives. This yields the key.

(b) Backwards compatibility: If a 3-DES computer communicates with a 1-DES computer, it can let $K_1 = K_2$ and get single encryption.