Homework 01 Solutions

ECE 443/518, Fall 2024

1. *(1 point)* Solve Problem 1.4 (p25 in Understanding Cryptography).

   Answer:

   1) 8 letters, each letter is 7 bit, which makes $8 * 7 = 56$bit, there will be 2^{56} different combination of keys.
   2) 56
   3) If we only use lowercase, there will be 26 options per letter. 8 letters make 26^8 different keys, equivalent to $\log_2 26^8 \approx 37.6$ bits.
   4) For 7-bit you will need $\lceil \frac{128}{7} \rceil = 19$ letters. For lowercase you will need $\lceil \frac{128}{\log_2 26} \rceil = 28$ letters.

2. *(1 point)*

   A. Calculate $2x$ mod 13 for $x = 1, 2, \ldots, 12$.

   B. Calculate $3x$ mod 13 for $x = 1, 2, \ldots, 12$.

   C. Argue that if p is a prime number and $1 \leq x < y \leq p - 1$ are two integers, then for any integer $1 \leq a \leq p - 1$, ax mod p and ay mod p cannot be the same.

   Answer:

   A. 2 4 6 8 10 12 1 3 5 7 9 11

   B. 3 6 9 12 2 5 8 11 1 4 7 10

   C. If they are the same then $ax - aymodp = 0$, which says $a|x - y|$ is a multiple of p. This is impossible since both a and $|x - y|$ are positive integers less than p.

3. *(1 point)*

   A. Calculate 2^x mod 13 for $x = 1, 2, \ldots, 12$.

   B. Calculate 3^x mod 13 for $x = 1, 2, \ldots, 12$.

C. What do the infinite sequences 2^x mod 13 and 3^x mod 13 look like for $x = 1, 2, \ldots,$?

Answer:

A. 2 4 8 3 6 12 11 9 5 10 7 1

B. 3 9 1 3 9 1 3 9 1 3 9 1

C. They are both periodic sequences with a period of 12.

4. *(0.5 point)* Solve Problem 2.4 (p52 in Understanding Cryptography).

   Answer: Just consider an example where the plaintext is BBBBB, i.e. 42 42 42 42 42 in ASCII/hex.

   For an OTP of 01 01 01 01 01, the ciphertext is 43 43 43 43 43, i.e. CCCCC. However, with just the ciphertext 43 43 43 43 43, it is also possible that the plaintext is AAAAA, i.e. 40 40 40 40 40, since the OTP key could be 03 03 03 03 03. In other words, without additional information regarding the plaintext, exhaustive key search is useless since every plaintext is possible and every key is possible.

5. *(0.5 point)* Solve Problem 4.16 (p121 in Understanding Cryptography).
   For Moore's Law, simply assume that computer power doubles every 18 months.

   Answer:

   1) There is a total of $2^{192} \approx 6.3 \times 10^{57}$ keys. One such IC will check $3 \times 10^7 \times 3600 \times 24 \times 365 \approx 10^{15}$ keys per year. 100000 IC will check 10^{20} keys per year so we would need 6.3×10^{37} years. This is far beyond the age of universe.
   2) To find the key in 24 hours we need our IC to be $6.3 \times 10^{37} \times 365 \approx 23 \times 10^{39} \approx 2^{134}$ times faster. That would need $134 \times 1.5 \approx 200$ years.

6. *(0.5 point)* Solve Problem 5.9 (p146 in Understanding Cryptography).

   Answer: $1TB = 2^{40}$ bytes so there will be 2^{36} 128-bit blocks. Therefore the counter has to be at least 36 bits and the IV is at most $128 - 36 = 92$ bits.

7. *(0.5 point)* Solve Problem 11.2 (p315 in Understanding Cryptography).

   Answer:

   1) If you can break the one-way property then you can recover the exact password from the hash. If you can find second preimages then you can log into the system with a different password. It won't help in this case if you can find collisions because you don't know the password.
   2) Salt helps if the attacker precompute hashes for popular password choices. No salt won't help if either the one-way property is broken or second preimages can be found.
   3) No. 80-bit seems too small to prevent finding second preimages.