Makeup Exam 1 Solutions

- **Group Members: Yu Wang(wangy52 661834351)**
- **Collaborators: no**

Problem 1

The code can be found in file "p1-collision-attack.py". The original text is

More efficient attacks are possible by employing cryptanalysis to specific hash functions. When a collision attack is discovered and is found to be faster than a birthday attack, a hash function is often denounced as "broken". The NIST hash function competition was largely induced by published collision attacks against two very commonly used hash functions, MD5 and SHA-1. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a few seconds on a regular computer. Hash collisions created this way are usually constant length and largely unstructured, so cannot directly be applied to attack widespread document formats or protocols.

By adding options to words using synonyms, paragraphs with the same meaning can be made using the followiong template:

{More efficient, High efficient} *attacks are* ***{possible, practical}*** *by* ***{employing, applying, using, making use of, exploiting, utilizing}*** *cryptanalysis to* ***{specific, perticular, certain}*** *hash functions. When a collision attack is* ***{discovered, uncovered}*** *and is* ***{found, realized, shown, proved}*** *to be faster, quicker than a birthday attack, a hash function is often* ***{denounced, declared, considered, regarded}*** ***{as, to be}*** *"broken". The NIST hash function competition was* ***{largely, mainly}*** ***{induced, inspired}*** *by published collision attacks against two very* ***{commonly, widely}*** *used hash functions,* ***{MD5 and SHA-1, SHA-1 and MD5}****. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a* ***{few, couple of}*** *seconds on a* ***{regular, common}*** *computer. Hash collisions* ***{created, generated}*** *this way are usually* ***{constant, fixed}*** *length and* ***{largely, almostly}*** *unstructured, so* ***{cannot directly, impractical to}*** *be* ***{applied, deployed, used}*** *to attack widespread document formats or protocols.*

Note that, choose one of the words in the bracket.

In all, there are

$$2 \times 2 \times 6 \times 3 \times 2 \times 4 \times 2 \times 4 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 3 = 28311552 \tag{1-1}$$

different permutations of the original text.

After exhaustive search, 64-bit and 128-bit hashing functions takes 249 and 24590 attempts respectively to encounter a collision. For 64-bit hashing, the two "similar" paragraphs are

More efficient attacks are possible by using cryptanalysis to perticular hash functions. When a collision attack is uncovered and is realized to be faster than a birthday attack, a hash function is often denounced as "broken". The NIST hash function competition was largely induced by published collision attacks against two very commonly used hash functions, MD5 and SHA-1. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a few seconds on a regular computer. Hash collisions created this way are usually constant length and largely unstructured, so cannot directly be applied to attack widespread document formats or protocols.

and

More efficient attacks are possible by applying cryptanalysis to specific hash functions. When a collision attack is uncovered and is found to be faster than a birthday attack, a hash function is often denounced as "broken". The NIST hash function competition was largely induced by published collision attacks against two

very commonly used hash functions, MD5 and SHA-1. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a few seconds on a regular computer. Hash collisions created this way are usually constant length and largely unstructured, so cannot directly be applied to attack widespread document formats or protocols.

Their hash values are both *69ae*.

For 128-bit hashing, the two "similar" paragraphs are

High efficient attacks are possible by making use of cryptanalysis to perticular hash functions. When a collision attack is uncovered and is shown to be faster than a birthday attack, a hash function is often declared to be "broken". The NIST hash function competition was largely inspired by published collision attacks against two very commonly used hash functions, MD5 and SHA-1. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a few seconds on a regular computer. Hash collisions created this way are usually constant length and largely unstructured, so cannot directly be applied to attack widespread document formats or protocols.

and

More efficient attacks are possible by employing cryptanalysis to certain hash functions. When a collision attack is discovered and is proved to be faster than a birthday attack, a hash function is often declared as "broken". The NIST hash function competition was largely induced by published collision attacks against two very commonly used hash functions, MD5 and SHA-1. The collision attacks against MD5 have improved so much that, as of 2007, it takes just a few seconds on a regular computer. Hash collisions created this way are usually constant length and largely unstructured, so cannot directly be applied to attack widespread document formats or protocols.

Their hash values are both *951a7950*.

Problem 2

10-12

x	x^3+2x+1	$QR(7)$	y
0	1	✓	1,6
1	4	✓	2,5
2	6	✗	N/A
3	6	✗	N/A
4	3	✗	N/A
5	3	✗	N/A
6	5	✗	N/A
∞	N/A	N/A	∞

Table 1: Table of X and y for $E_7(2,1)$

So all the points in $E_7(2,1)$ are $\{(0,1),(0,6),(1,2),(1,5),(\infty,\infty)\}$.

10-13

$$-P=(3,-5)=(3,2)$$
$$-Q=(2,-5)=(2,2)$$
$$-R=(5,0)$$

10-14 Honestly, I write a program and use the program to generate all the points. The code is in "p2-10-14-ECC.py"

1G	(3, 2)	2G	(10,4)
3G	(1,8)	4G	(5,4)
5G	(4,8)	6G	(7,7)
7G	(6,8)	8G	(6,3)
9G	(7,4)	10G	(4,3)
11G	(5,7)	12G	(1,3)
13G	(10,7)	14G	(3,9)

10-15 All the computations can be found in the code titled "p2-10-15-ECC.py".

(a)

$$P_B = n_B G = 7 \times (3, 2) = (6, 8) \tag{2-1}$$

(b) Note that $C_m = [kG, P_m + kP_B]$.

$$kG = 5G = 5 \times (3, 2) = (4, 8) \tag{2-2}$$
$$P_m + kP_B = (10, 7) + 5 \times (6, 8) = (1, 8) \tag{2-3}$$

(c) For decryption, $P_m = P_m + kP_B - n_B(kG)$.

$$P_m = (1, 8) - 7 \times (4, 8) = (1, 8) - (4, 8) = (1, 8) + (4, -8) = (10, 7) \tag{2-4}$$

Problem 3

All the codes can be found in file "p3-primality$_a nd_f actorization.py''$

(a)

After running the Miller-Rabin Algorithm to each number and 1000 rounds each, we find that 31531, 485827 and 15485863 are prime and 520482 is composite.

(b)

Applying Pollard-Rho method to 520482 and we find that it has a factor 3

$$520482 = 2 \times 3 \times 223 \times 389. \tag{3-1}$$