Final Exam

Instructions: This is a closed book exam with 4 pages of problems. Do all problems. You are allowed one letter-sized page of handwritten notes. No electronic devices are allowed. Communicate your ideas ***clearly*** and ***succinctly***. Show all work. Good luck!

Your name and class ID:

Your email (in case I have a question):

On problem	you got	out of
1		4
2		6
3		5
4		5
5		5
6		5
7		5
8		5
9		5
10		5
11		5
12		5
Σ		60

1) Let's say f is a function that takes a two-byte input and produces a two-byte output. How many different functions f have this same function signature? Explain very briefly.

How many different invertible functions f have this same function signature? Explain very briefly.

---

2) Below is Horner's method of polynomial evaluation with four different variations. For each variation write the equivalent polynomial. Write "..." to indicate "the pattern continues until", and use x_i instead of $x[i]$. *Hint: The first one is* $x_0 k^n + x_1 k^{n-1} + \cdots + x_{n-1} k$.

```
                        A      B           C                    res
res = A
                        0  res + x[i]  res * k     ________________________________________
for (i=0; i<n; i++)
                        0  res * k     res + x[i]  ________________________________________
    res = B
                        1  res + x[i]  res * k     ________________________________________
    res = C
                        1  res * k     res + x[i]  ________________________________________
```

---

3) AES uses GF(256). What are the values $01010101_2 + 00010001_2$ and $01010101_2 \times 00010001_2$ when computed using GF(256)? The polynomial used in AES is $x^8 + x^4 + x^3 + x + 1$.

4) You are given a black box f that takes 8-bit inputs and returns 8-bit outputs. It is either a random function or a random permutation. You are allowed 3 queries of f. Give a distinguishing algorithm that maximizes advantage, and evaluate what the advantage is.

---

5) Calculate $7^{-1} \bmod 60$ using Euclid's Extended Algorithm (egcd).

---

6) You decide to RSA encrypt the grade that you think you should get in this class (A=4, B=3, C=2). In generating your keys, you pick $p = 11$ and $q = 7$. Complete the generation of public and private keys, then encrypt your grade. Explain briefly what you are doing in each step.

7) Let's say you had a 128-bit random string X, but you wanted a 1000-bit string Y that looks random. How could you produce 1000 bits using any of the cryptographic primitives seen in this class? Give your answer in pseudocode.

---

8) What is `0xAAAA` mod $2^8 - 2$? Compute your answer using divisionless modular reduction.

---

9) Answer true of false for each of the following. For each false write what you believe is a true version of the statement.

AES256 block size is 256 bits.

AES128 key size is 128 bits.

RSA key sizes are thousands of bits.

Elliptic curve key sizes are thousands of bits.

Preimage resistance implies collision resistance.

Diffie-Helman cannot be used for encryption.

You need $O(n^2)$ public keys for n parties to communicate with each other.

Cryptographic hash functions are faster than almost-universal hash functions.

10) Let `p(x) = ROTL1(x)` be a permutation on four bits (rotate `x` left one bit). Let's say you receive the CBC ciphertext `1101 1001 1110 0010`. What is the original message? The message was encrypted using `p`, 10* padding, and the IV is the first four bits of the ciphertext.

---

11) The 4-bit primes are 11 and 13. The 6-bit primes are 37, 41, 43, 47, 53, 59 and 61. Find 6-bit prime p and value $g \in \mathbb{Z}_p^*$ where g generates a subgroup whose size is a 4-bit number. Explain briefly what you are doing in each step.

---

12) Calculate 2^{50} mod 11 using the method learned in class. Show your work. ($50_{10} = 110010_2$.)