Q1(30 points): Confidentiality and Integrity

Suppose that host $A$ and $B$ are connected by insecure public networks. Assume that $A$ and $B$ have synchronized system time. Let $M$ be a plaintext message and $K$ be a secret key shared by $A$ and $B$. Let

- $CBC(X, K)$ denotes the ciphertext of a plaintext $X$ after a secret key encryption (CBC mode) using a key $K$.
- $MD(X, K)$ denotes the message digest of a plaintext $X | K$.
- $RSA(X, I)$ denotes the ciphertext of a plaintext $X$ after an RSA public key operation using $I$’s public key.
- $RSA\{X, I\}$ denotes the ciphertext of a plaintext $X$ after an RSA private key operation using $I$’s private key.

If $A$ sends out a packet to $B$ that the packet’s headers encapsulate one of the following.

1. $CBC(M + timestamp, K)$ and IV.
2. Residue of $CBC(M + timestamp, K)$, $M$ and IV.
3. $CBC(M + A’s \ IP \ address, K)$ and IV.
4. $MD(M, K)$.
5. $MD(M + A’s \ IP \ address, K)$ and $M$.
6. $MD(M + timestamp, K)$ and $M$.
7. $RSA\{M + timestamp, A\}$ and $M$.
8. $RSA(M + timestamp, B)$.

(a)(10 points) Please list the numbers above to indicate which packets achieve the security goal confidentiality.

(b)(10 points) Please list the numbers above to indicate which packets achieve the security goal integrity.

(c)(10 points) Please list the numbers above to indicate which packets achieve the security goal authenticity.
• Q2(15 points): Public key certificates

Alice is in a security domain under a public key certificate authority $CA_a$, whereas Bob is in another security domain under another certificate authority $CA_b$. Assume both $CA_a$ and $CA_b$ trust each other and they have certified each other’s public keys. Furthermore, both $CA_a$ and $CA_b$’s public keys are publicly known to the entities in their own domains. Now, if Alice would like to request and verify Bob’s public key,

(a)(6 points) How many and what public key certificates Alice needs to collect?

(b)(9 points) With the collected public key certificates in part (a), in order to verify Bob’s public key, what is the sequence of steps that Alice needs to do?
Q3 (20 points): Cryptology

(a) (10 points) Given a prime elliptic curve $E_{23}(1, 1)$, i.e., $y^2 \mod 23 = x^3 + x + 1 \mod 23$, there are two points $P = (17, 20)$ and $Q = (9, 7)$ on the curve. Please find another point $R$ on the curve, where $R = P + Q$.

(b) (10 points) In an elliptic curve cryptosystem, multiplying a scalar number $k$ to a point $G$ on a curve $E_p(a, b)$ will result in another point $Q$ on the curve. That is $Q = k \cdot G$, where both $G, Q \in E_p(a, b)$.

Now given a point $G$ and $k = 103$, how many elliptic curve additions are required to compute $Q = 103 \cdot G$?
• Q4(10 points): Buffer Overflow/format String Vulnerability

```c
int main(int argc, char *argv[]) {
    char buff[50];

    if (argc < 2) {
        printf("Syntax: %s <input string>\n", argv[0]);
        exit(0);
    }

    strcpy(buff, argv[1]);
    return 0;
}
```

Assume you are an attacker, you can exploit the buffer overflow vulnerability of above codes. In addition to crash the program, can you gain the control of the program to execute arbitrary codes and how?
• Q5 (10 points): SQL Injection

The following SQL query that requires user input could be vulnerable to SQL Injections.

SELECT fname, lname FROM employee WHERE ssn = 'user input';

Assume you are an attacker, please provide a user input that may maliciously cause an employee “John Smith” to be removed from the employee table.