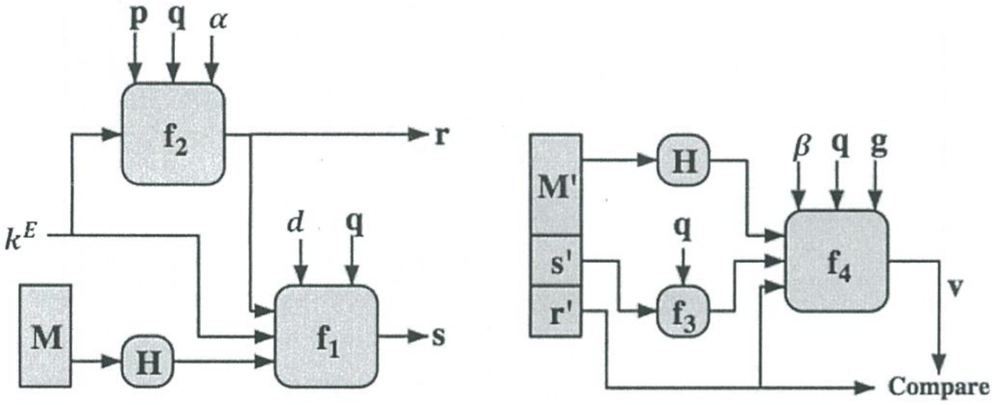
Final Exam of Introduction to Information Security (110 points)

Type I: calculation (45 points)

1. (10 points) Consider an ElGamal scheme between Alice and Bob with a common prime $q = 67$ and a primitive root $\alpha = 9$.
   (a) If Bob has public key $Y_B = 14$ and Alice chooses the random integer $k = 3$, what is the ciphertext of $M = 20$?
   (b) If Alice now chooses a different value of k so that the encoding of $M = 20$ is $C = (62, C_2)$, what is the integer C_2?

2. (10 points) Suppose Alice and Bob use a DSA with a common prime $p = 59$, $q = 29$, primitive root $\alpha = 3$ and privatw key $d = 7$
   (a) If Bob has Plaintext x ,ephermal key $k_E = 9$ and compute hash of message $H(x) = 10$, what is the r and s ?
   (b) If Alice have $(x, (r, s))$ that is from the Bob. Please use the $(x, (r, s))$ to verify that x is real from the Bob.



$$s \equiv (\mathrm{SHA}(x) + d \times r)k_E^{-1} \bmod q$$
$$r \equiv (\alpha^{k_E} \bmod p) \bmod q$$

(a) Signing

$$w \equiv s^{-1} \bmod q$$
$$v \equiv (\alpha^{w\mathrm{SHA}(x) \bmod q} \times \beta^{wr \bmod q} \bmod p) \bmod q$$

(b) Verifying

3. (10 points) Please calculate x in $3^x = 76 \bmod 139$ by using Baby-Step-Giant-Step method.

4. (10 points) Suppose Alice and Bob use a Diffie-Hellman Key Exchange with a common prime $p = 17$ $\alpha = 5$, Alice's private key = 7 and Bob's private key = 11. Please compute their common secret key.

5. (5 points) Using Little Fermat's theorem, find $7^{254} \bmod 17$.

Type II: answer questions (70%)

6. (10 points) Please describe the two different kinds of implementations in MACs.
7. (10 points) Please describe how to identify the gmail website is valid when you using web browser like

chrome/IE/Firefox? (hint: challenges/response)

8. (10 points) Please describe how CRT helps RSA achieve fast decryption.
9. (10 points) Please describe the speed up process of ElGamal.
10. (5 points) Please describe how Man-in-the-Middle attack works in DH key Exchange procedure.
11. (5 points) Please explain why Fermat's Test fails for primality.
12. (5 points) What's the birthday paradox? And what is its meaning for hash function?
13. (5 points) RSA Digital Signature seems popular and very secure. In this case, why we use DSA for digital signature? Please explain the main advantage of DSA.
14. (5 points) What's the typical value of public key in RSA? What's the advantage of it?