1. Try to use the EVP framework function of the OPENSSL library to describe the process of making a digital envelope by the national secret algorithm SM2.

2. Assume that in the RSA public key cryptosystem p=31, q=29, encryption key e=17,

(1) Try to find the decryption key based on the encryption key d.

(2) If the cipher text is c=58, try to plaintext. (all require writing process,

3. Let H be a 128-bit HASH function. The R1, R2, and R3 functions inversely map the 128-bit hash value to a 6-character password. Using H and 3 R functions, a rainbow chain of length 3 can be formed:

$$pass0 \xrightarrow{H} h1 \xrightarrow{R1} pass1 \xrightarrow{H} h2 \xrightarrow{R2} pass2 \xrightarrow{H} h3 \xrightarrow{R3} pass3$$

The pass0, pass1, pass2, and pass3 are all strings of length 6. The characters range from 10 digits to 26 lowercase letters. Question: If 10^7 such rainbow chains are generated (pass0 are different from each other), how many different chain tails (pass3) are there?

4. Proof of proof: the plaintext space is the encryption scheme Π = (Gen, Enc, Dec) for any probability distribution on M, any plaintext m $\in$ M and any ciphertext c $\in$ X and Pr[C=c]>0, and Pr [M = m | C = c] = Pr [M = m] only when there is $\Pr[\Pr ivK_{A,\Pi}^{eav} = 1] = \frac{1}{2}$ for all adversary A.

5. Consider a password scheme where $\mathrm{M} = \{a, b, c\}, \mathrm{C} = \{1, 2, 3\}, \mathrm{K} = \{K_1, K_2\}$. Assume that the encryption matrix is as follows:

	a	*b*	*c*
K_1	3	2	1
K_2	1	3	2

If $\Pr[K_1] = \frac{1}{2}, \Pr[K_2] = \frac{1}{2}, \Pr[a] = \frac{1}{2}, \Pr[b] = \frac{1}{4}, \Pr[c] = \frac{1}{4}$

a) Try to determine if the password scheme is perfect and confidential. (3 points)

b) Explain whether it is possible to change the integrity of the cryptographic scheme by adjusting the distribution of plaintext.