Question 1. Hashing (6 + 7 + 7 = 20 points)

Let **n**=**p**x**q** be a public **RSA** modulus such that **p** ≡ **q** ≡ 3 (mod 4). Consider the function

$$\mathbf{SQ}(\mathbf{x}) = \min\{\ \mathbf{x}^2 \ \underline{\text{mod}}\ \mathbf{n}\ ,\ \mathbf{n}\text{-}\mathbf{x}^2\ \underline{\text{mod}}\ \mathbf{n}\ \}$$

where $0 < \mathbf{x} < \mathbf{n}/2$.

a) Show that **SQ** is two-to-one over $\{1, \ldots, (\mathbf{n}-1)/2\}$. Why use **p** ≡ **q** ≡ 3 (mod 4)?

b) Show that, as a hash function, **SQ** is collision resistant unless **p** and **q** can be found.

c) For a 1025-bit **n**, explain how we may create from **SQ** a collision resistant hash function **SQ'**: $\{0,1\}^* \rightarrow \{0,1\}^{1024}$ that is collision resistant unless **p** and **q** can be found.

Question 2. 3F-AES (10 + 10 = 20 points)

Consider the 256-bit block cipher **3F-AES** obtained by combining three (independent) instances of **AES** in a 3-round Feistel network. The total key-size of this new cipher is 384 bits.

I. Let **m** be a 256-bit message and **k** be a 384-bit key. Give an explicit formula for the encryption/decryption functions of **3F-AES** (you may invoke **AES** as a black-box).

II. Discuss the pseudo-random nature of the permutation defined by **3F-AES**.

Question 3. Operations à la mode (6 + 7 + 7 = 20 points)

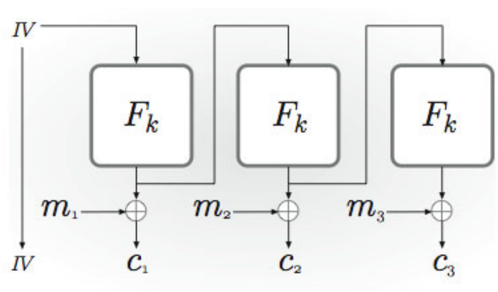

FIGURE 3.7: Output Feedback (OFB) mode.

Remember the **OFB** mode of operation for block ciphers.

(i) Draw a similar figure to explain decryption of **OFB** encrypted cipher-text $\langle IV, c_1, c_2, c_3, \ldots \rangle$.

(ii) Why is **OFB** not suitable to use with a Public-key crypto-system ?

(iii) Suggest a modification of **OFB** mode that would make it suitable to use with a Public-key crypto-system (assuming $\boldsymbol{F_k}$ is an invertible block cipher) ?

Question 4. Mac vs Signature (6 + 6 + 8 = 20 points)

I. Explain why the term "*Signature*" is only used for the *public-key* setting.

II. Explain why textbook **RSA** is NOT existentially unforgeable.

III. We know it is possible to have **MAC**s that are secure without computational assumptions. Why not signatures ?

Question 5. Pseudo-random Mac (10 + 10 = 20 points)

CONSTRUCTION 3.17

Let G be a pseudorandom generator with expansion factor ℓ. Define a private-key encryption scheme for messages of length ℓ as follows:

- Gen: on input 1^n, choose uniform $k \in \{0,1\}^n$ and output it as the key.
- Enc: on input a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^{\ell(n)}$, output the ciphertext
$$c := G(k) \oplus m.$$
- Dec: on input a key $k \in \{0,1\}^n$ and a ciphertext $c \in \{0,1\}^{\ell(n)}$, output the message
$$m := G(k) \oplus c.$$

A private-key encryption scheme based on any pseudorandom generator.

Construction 3.17 above was used in class to obtain a private-key encryption scheme from any pseudo-random generator *G*.

i) Provide a similar construction to obtain a **MAC** scheme from any pseudo-random generator. Use the same level of details as the above construction.

ii) Argue that if the generator *G* is pseudo-random then your **MAC** scheme will be existentially unforgeable under an adaptive chosen-message attack.

Write the word for 5 bonus points…