McGill

DECEMBER 2009
Final Examination

FINAL EXAMINATION

Computer Science COMP-547A
Cryptography and Data Security

7 DECEMBER 2009, 9h00

Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Prof. David Avis

INSTRUCTIONS:

- This examination is worth 50% of your final grade.
- The total of all questions is 100 points.
- Each question heading contains (in parenthesis) a list of values for each sub-questions.
- This is an **open book** exam. **All documentation is permitted.**
- Faculty standard calculator permitted only.
- The exam consists of 5 questions on 4 pages, title page included.

Suggestion:

read all the questions and their values before you start.

Question 1. Elgamal (10+5+5+5 points)

A) Given an Elgamal public-key $pk = \langle \mathbb{G}, q, g, h \rangle$, assume there exists an adversary A running in time t_A for which

$$\Pr[\, A(\, ENC_{pk}(x)\,) = x \,] = 0.01$$

where the probability is taken over random choice of $x \leftarrow \mathbb{G}$ (to put it differently, **1%** of the x have encryptions that are easy to break). Assume also that there exists an algorithm D to solve the **DDH** problem over $\mathbb{G}$ running in time t_D. Show that it is possible to construct a probabilistic adversary A' for which

$$\Pr[\, A'(\, ENC_{pk}(x)\,) = x \,] = 0.99$$

for all $x \in \mathbb{G}$, where the probability is solely taken over the random choices of A' (to put it differently, the encryption of any x can be broken with probability **99%**). The running time t' of A' should satisfy $t' = \mathrm{poly}(\|q\|, t_A, t_D)$.

B) Consider an alternative to El Gamal encryption. Imagine that the new scheme has the same public key $pk = \langle \mathbb{G}, q, g, h = g^a \rangle$ for some private a. However the encryption adds the message instead of multiplying it in, this means that an encryption of m would be a pair (c_1, c_2) where $c_1 = g^y$ and $c_2 = h^y + m$ for some random $y \in \mathbb{Z}_q$.

(i) Describe the decryption algorithm of this alternate scheme.

(ii) Compare the security of the alternate scheme with the security of the original scheme.

(iii) Explain advantages and disadvantages to this alternate method.

Question 2. AES secure message transmission (20 points)

Start with 128-bit AES (block and key lengths) and construct a secure message transmission scheme for messages of arbitrary length (at most 2^{128} bits). Build everything from CBC-mode. Provide all the details (definition of secure message transmission, instantiation of all components using CBC-mode of AES).

Question 3. Short and sweet (5+5+5+5 points)

5.5 What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

(a) Each round function outputs all 0s, regardless of the input.

(b) Each round function is the identity function.

7.6 Compute $[101^{4,800,000,023} \bmod 35]$ (by hand).

7.13 Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

Question 4. Operations à la mode (5+5+5 points)

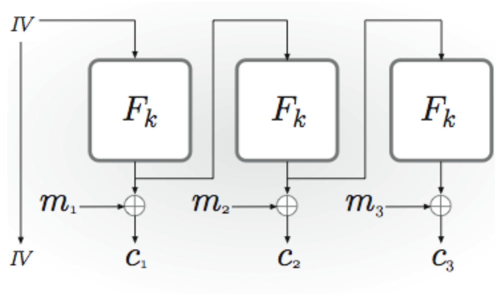

FIGURE 3.7: Output Feedback (OFB) mode.

A) Remember the OFB mode of operation for block ciphers.

(i) Why is OFB not suitable to use with a Public-key cryptosystem ?

(ii) Can you suggest a modification of OFB mode that would make it suitable to use with a Public-key cryptosystem (assuming $\boldsymbol{F_k}$ is a clock cipher) ?

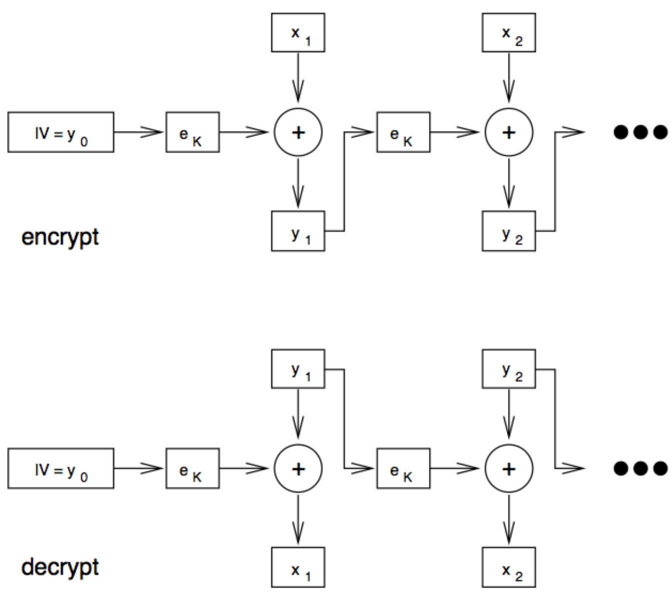

FIGURE 3.10
CFB mode

B) Consider an alternative mode of operation for block ciphers called Cipher FeedBack (CFB) as in the figure above.

(i) Explain whether this mode of operation is suitable for use as a message authentication code as was done with CBC mode.

Question 5. MAC vs ENC (5+5+5+5 points)

A) We saw in class and in the notes that private-key authentication can be used to implement private-key encryption.

i) Explain precisely why this implication fails in the public-key scenario.

ii) In the private-key scenario, assume we start with an authentication scheme existentially unforgeable under an adaptive chosen-message attack to construct an encryption scheme as we saw in the notes. What level of security will the resulting encryption scheme be ??

B)

CONSTRUCTION 3.15

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 $k \leftarrow \{0,1\}^n$ uniformly at random 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 plaintext message
$$m := G(k) \oplus c.$$

A private-key encryption scheme from any pseudorandom generator.

The construction above was used in class to obtain a private-key encryption scheme from any pseudo-random generator.

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 is pseudo-random then your MAC scheme will be existentially unforgeable under an adaptive chosen-message attack