UNIVERSITY OF BRISTOL

JANUARY 2016 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

Answers to COMS-30002(J): CRYPTOGRAPHY A

Intended Learning Outcomes:

On successful completion of this unit you will be able to

1. understand the Mathematical underpinnings of cryptography,
2. appreciate and apply appropriate cryptographic proofs of security,
3. understand the design and operation of standard, state-of-the-art symmetric and asymmetric cryptographic schemes,
4. appreciate basic cryptanalytic techniques, and apply this knowledge to problems such as selection of key size.

Q1. For each of the following statements decide whether it is true or false, and write down the correct answer in the exam book. Provide a short justification for each answer.

(a) Perfect secrecy of the One-Time Pad implies that the key can be reused securely.

[3 marks]

Solution: False, security breaks down badly if the key is reused. For instance the xor of two ciphertexts will reveal the xor of the corresponding plaintexts.

(b) CTR mode using AES-128 is IND-CCA secure.

[3 marks]

Solution: False, various attacks can be given to demonstrate this.

(c) A single round of the Feistel construction does not suffice for a secure blockcipher.

[3 marks]

Solution: True, half the plaintext is simply copied without modification into the ciphertext.

(d) For a *deterministic* public key encryption scheme, OW-CCA security does not imply OW-CPA security.

[3 marks]

Solution: False. One can give a quick reduction, or simply observe that a CCA adversary has at least as much power as a CPA adversary (irrespective of goal and scheme), so CCA will always imply CPA security.

(e) Cryptology is not used in practice.

[3 marks]

Solution: False, many examples can be given where crypto is used (TLS, EMV, AES-NI).

Q2. This question focuses on a variant of the RSA cryptosystem.

Key generation Kg selects three random yet distinct 767-bit prime numbers p', q', and r' such that $p \leftarrow 2p' + 1, q \leftarrow 2q' + 1$, and $r \leftarrow 2r' + 1$ are all prime as well. Let $N \leftarrow p \cdot q \cdot r$. Set $e \leftarrow 3$ and set d to the smallest positive integer such that the least common multiple $\mathrm{lcm}(p-1, q-1, r-1)$ divides $d \cdot e - 1$. Publish (N, e) as the public key pk and keep (N, d) as the private key sk.

Encryption Enc takes as input the public key $\mathsf{pk} = (N, e)$ and a message $\mathsf{m} \in \mathbb{Z}_N$. It computes and returns ciphertext $\mathsf{c} \leftarrow \mathsf{m}^e \bmod N$.

Decryption Dec takes as input a private key $\mathsf{sk} = (N, d)$ and a ciphertext $\mathsf{c} \in \mathbb{Z}_N$. It computes and returns $\mathsf{m}' \leftarrow \mathsf{c}^d \bmod N$.

(a) Prove correctness of the scheme.

[5 marks]

Solution: We know that $\mathrm{lcm}(p-1, q-1, r-1)$ divides $d \cdot e - 1$, so we can write $d \cdot e = 1 + k \cdot \mathrm{lcm}(p-1, q-1, r-1)$. Correctness requires us to show that encrypting then decrypting returns the original message. That is, for all $\mathsf{m} \in \mathbb{Z}_N$ we need to show that $(\mathsf{m}^e)^d \bmod N = \mathsf{m}$. Since $N = p \cdot q \cdot r$ we may equivalently show that $\mathsf{m}^{d \cdot e} \bmod x \equiv \mathsf{m}$ for $x \in \{p, q, r\}$. Substituting the formula for $d \cdot e$ leads to $\mathsf{m}^{1+k \cdot \mathrm{lcm}(p-1,q-1,r-1)} \bmod x \equiv \mathsf{m}$. If $\mathsf{m} \equiv 0 \bmod x$, this is immediate, whereas if $\mathsf{m} \not\equiv 0 \bmod x$, then it is invertible modulo x (since $x \in \{p, q, r\}$ is prime) so the statement simplifies to $\mathsf{m}^{k \cdot \mathrm{lcm}(p-1,q-1,r-1)} \bmod x \equiv 1$ which is true as m will have order dividing $p - 1$ (Fermat, Euler, or Lagrange) and the exponent $k \cdot \mathrm{lcm}(p-1, q-1, r-1)$ is a multiple of $p - 1$ and thus also of the order of m.

Marking: 1 point for rephrasing the $d \cdot e$ relation, 1 point for expressing what correctness entails in this scenario, 1 point for applying CRT style technique, 1 point for mostly correct use of Fermat, 1 point for taking care of $\mathsf{m} \equiv 0$ case.

(b) Discuss the strengths and weaknesses of the encryption scheme. Mention at least three distinct ones (strengths and weaknesses combined). Illustrate with attacks where appropriate (no reductions are required).

[5 marks]

Solution: The picture is exactly as for vanilla RSA, albeit with OW-CPA security based on a slightly adapted assumption (using 3-prime moduli instead of the usual 2). The scheme is not IND-CPA as demonstrated by the standard attack against any deterministic scheme, the scheme is not IND-CCA as demonstrated by the standard attack against any homomorphic scheme. The exponent $e = 3$ enables multi-user attacks (CRT based on 3 users), or attacks against OW-CPA in case the message is not chosen uniformly at random, but instead from $\{0, \ldots, 2^{768}\}$ (as there is no modular wrap around).

Marking: 1 mark per observation and 1 mark per justification; with a maximum of 5.

(c) Describe how you would build an EUF-CMA signature scheme related to this encryption scheme by specifying the relevant algorithms for key generation, signing, and verification.

[3 marks]

Solution: FDH using the TDP from above.

(cont.)

Marking: 1 mark for each correct algorithm. Describing vanilla-RSA sigs instead gives 1 point.

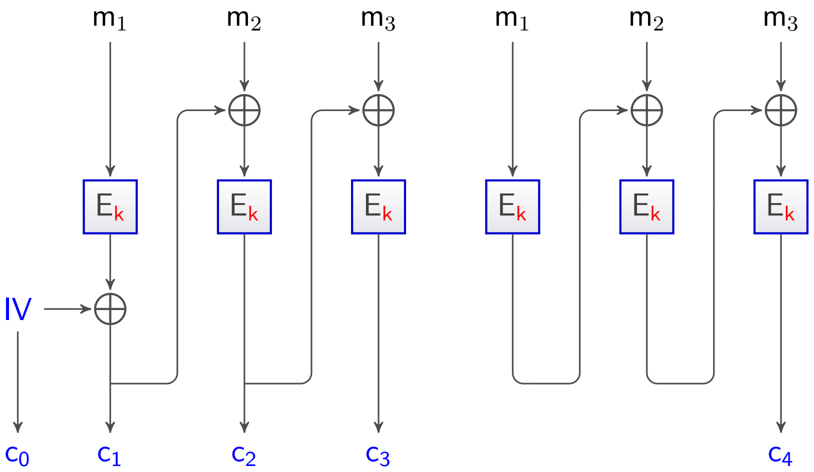
(d) Under what assumption(s) would your signature scheme be EUF-CMA secure (no reduction required)?

[2 marks]

Solution: Modified RSA assumption in the random oracle model.

Marking: 1 point for each.

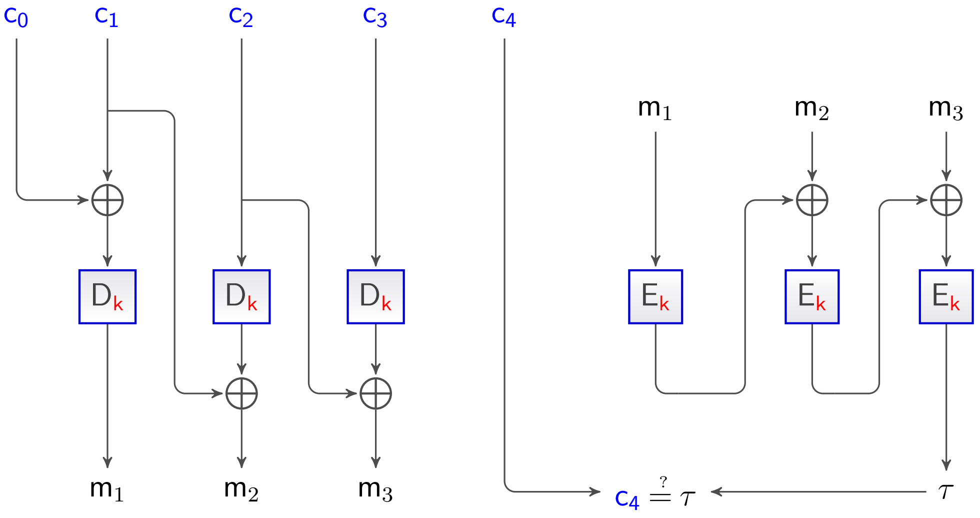
Q3. This question asks you to evaluate the security of an authenticated encryption scheme. The scheme is based on combining CBC-style encryption and authentication, both based on DES. Let E denote the encryption algorithm of the DES blockcipher. For key generation, generate a single DES key k that will be used throughout. To encrypt a three block message $(\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$, generate a random initial vector IV and output the ciphertext $(\mathsf{c}_0, \ldots, \mathsf{c}_4)$ with the computation according to the diagram below. Here the final block of ciphertext c_4 is used as an authentication tag. The scheme generalizes to messages of an arbitrary number of blocks in the natural way.



(a) Describe what decryption would look like for this scheme. Base your decryption algorithm on ciphertexts corresponding to 3-block messages (as above).

[3 marks]

Solution:



Decryption first computes an unverified plaintext $(\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$, then recomputes the tag τ and only if it matches the ciphertext's tag c_4 it outputs the (by now verified) plaintext $\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$. If $\mathsf{c}_4 \neq \tau$, decryption returns $\perp$.

Marking: 1 point for correct calculation of $(\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$, 1 point for correct calculation of τ, 1 point for correct logic concerning $\perp$.

(b) Point out as many dubious design decisions of the scheme as you can. For each shortcoming, you should identify as clearly as possible which part of the scheme you are referring to, explain how and why security (or efficiency) suffers by presenting attacks (or referring to taught material), and suggest a remedy. You can obtain up to four points per shortcoming.

[12 marks]

Solution:

1. DES only has a 56-bit key, which is too short to provide effective security. It can be recovered using exhaustive search or, more likely against dedicated adversaries, using time–memory trade-offs. An obvious solution would be to use a modern 128-bit key blockcipher such as AES instead. 3DES as alternative is acceptable as well.

2. The IV is added at the wrong place (compared to CBC mode). As is, the mode is not IND-CPA secure. An adversary can first ask for the encryption of say (0) obtaining $(\mathsf{c}_0, \mathsf{c}_1, \mathsf{c}_2)$ and then submit the challenge (0) versus (1), resulting in challenge ciphertext $(\mathsf{c}_0^*, \mathsf{c}_1^*, \mathsf{c}_2^*)$. If $\mathsf{c}_0 \oplus \mathsf{c}_1 = \mathsf{c}_0^* \oplus \mathsf{c}_1^*$ then challenge (0) was likely encrypted, otherwise (1). One can remedy this by moving the xor of the initial vector up (so it occurs before the first blockcipher call).

3. The scheme uses encrypt-and-mac, which is not a secure type of composition. In particular, given a challenge ciphertext $(\mathsf{c}_0, \mathsf{c}_1, \mathsf{c}_2)$ one can easily create an alternative, valid ciphertext for the same message (block) by $(\mathsf{c}_0 \oplus x, \mathsf{c}_1 \oplus x, \mathsf{c}_2)$ for arbitrary (non-zero) block x. This observation immedialy implies an easy OW-CCA attack. Instead, authenticating the ciphertext (including the IV) through encrypt-then-mac is secure.

4. Encryption and authentication use the same key, which can lead to bad interaction. In this particular case, a ciphertext forgery is possibly without a single query, as $(0, \mathsf{c}_1, \mathsf{c}_2, \mathsf{c}_3, \mathsf{c}_3)$ is a valid ciphertext (for some unknown message). The solution is to use independent keys for providing confidentiality and authentication (or a mode-of-operation that is explicitly designed to cope with a single key, but these are not taught as part of the unit).

5. (semi-taught) DES only has a 64-bit block size, which is quite small when collision attacks are concerned. An adversary could ask for roughly 2^{32} encryptions of relatively long messages (say 10 blocks long), find two colliding tags, ask for the encryption of one of the messages truncated by one block, then construct a (likely) valid ciphertext for the other message truncated by one block (by truncating its original ciphertext by two blocks and then append the final block of the ciphertext of the other truncated message).

6. (not taught) CBC mode is susceptible to all sorts of block-wise or chosen-IV attacks.

7. (not taught) This mode only operates on messages whose length is a multiple of the block length, which is slightly restrictive. Especially for short messages the computational overhead is quite large.

Marking: For each shortcoming: 1 point for identification, 1 point for justification, 1 point for mitigation, plus 1 point for peachyness (giving a particularly pertinent, explicit, accurate, and concise answer). With a maximum of 12 points.

Q4. This question addresses an ElGamal-like cryptosystem. Assume G_q is a given group of (known) prime order q with public generator g. Consider the following algorithms defining key generation and encryption of the EGL cryptosystem.

Key generation Kg randomly generates a second generator f and selects two exponents x_1 and x_2 uniformly at random from $\mathbb{Z}_q$. Compute $y \leftarrow f^{x_1} g^{x_2}$. The public key comprises $\mathsf{pk} = (f, y)$ and the private key $\mathsf{sk} = (x_1, x_2)$.

Encryption Enc takes as input a public key $\mathsf{pk} = (f, y)$ and a message $m \in \mathsf{G}_q$. It randomly selects $r \in \mathbb{Z}_q$ and computes $c_1 \leftarrow f^r, c_2 \leftarrow g^r$ and $c_3 \leftarrow m \cdot y^r$. The ciphertext is (c_1, c_2, c_3).

(a) Describe a suitable decryption algorithm for the EGL cryptosystem.

[3 marks]

Solution: Dec takes as input a private key $\mathsf{sk} = (x_1, x_2)$ and a ciphertext (c_1, c_2, c_3). It computes and returns $m' \leftarrow c_3 \cdot c_1^{-x_1} c_2^{-x_2}$.

(b) Show that the EGL cryptosystem is homomorphic.

[2 marks]

Solution: Let ciphertext $(c_1, c_2, c_3) = (f^r, g^r, my^r)$ be an encryption of m and ciphertext $(c_1', c_2', c_3') = (f^s, g^s, m'y^s$ be an encryption of m'. Then $(c_1c_1', c_2c_2', c_3c_3') = (f^{r+s}, g^{r+s}, mm'y^{r+s})$ is an encryption of mm'.

(c) Under an appropriate assumption, either show that the EGL cryptosystem is OW-CPA or IND-CPA secure (your choice; both are possible). Clearly describe both the security notion and the assumption and explain how you set up your reduction, before fleshing out the details.

[10 marks]

Solution:

Marking: 2 points for bookwork definitions of a security notion and 3 points for the assumption (either CDH or DDH). 1 point for the correct security statement. 2 points for setting up the reduction and 2 points for its execution.

END OF PAPER