UNIVERSITY OF BRISTOL

JANUARY 2018 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. explain and apply the principles of modern cryptology in teh context of secure communication
2. explain and demonstrate the functionality and desired security of standard cryptographic schemes used for confidentiality and authenticity.
3. link the design and operation of standard, state-of-the-art symmetric and asymmetric cryptographic schemes to their mathematical underpinnings.
4. use basic cryptanalytic techniques to evaluate the security level of simple cryptographic schemes.

Q1. For each of the questions below, four possible answers are presented. Select *all* the answers that you believe apply, or write “none” if you believe none apply. You do not need to justify your answer.

For each question, you can receive up to 3 points, with 3 points only for the perfect answer and one point deducted per incorrect classification, to a minimum of 0 points per question (e.g. if the correct answer is “A and B” then answering “B” leads to 2 points, whereas answering “B and C” only leads to 1 point).

[15 marks]

(a) Which of the following modes most closely mirrors the one-time pad?

A. CTR
B. CBC
C. CFB
D. OFB

Solution:

A. True

B. False

C. False

D. True

(b) Which of the following statements is accurate?

A. AES is an SP Network
B. AES is a Feistel cipher
C. AES is an iterated cipher
D. AES uses key-whitening

Solution:

A. True, AES’s S-boxes (`SubBytes`) constitute the substitution layer, with `ShiftRows` and `MixColumns` being the permutation layer.

B. False, SP-Networks and Feistel ciphers are alternative design strategies. DES is a Feistel cipher.

C. True, SP Networks are a special case of an iterated cipher.

D. True, AES xors the key at the very beginning, as well as at the very end. Consequently, the number of subkeys is one higher than the number of rounds.

(c) In the sentences below, “harder than” should be interpreted as “known to be equally hard as or strictly harder than”.

A. Solving the DDH problem is harder than solving DLP
B. Solving the DDH problem is harder than solving the CDH problem
C. Solving the CDH problem is harder than solving DLP
D. Solving DLP is harder than solving the DDH problem.

Solution:

A. True

B. True

C. True

D. False

(d) Which of the following schemes are homomorphic?

A. Vanilla ElGamal
B. Vanilla RSA Encryption
C. RSA-OAEP
D. Hybrid ElGamal

Solution:

A. True

B. True

C. False

D. False

(e) The Chinese Remainder Theorem is commonly used to speed up

A. RSA encryption
B. RSA decryption
C. ElGamal encryption
D. ElGamal decryption

Solution:

A. False

B. True

C. False

D. False

Q2. The one-time pad can be proven to be perfectly secret.

(a) Describe the three algorithms Kg, Enc, and Dec of the one-time pad.

[3 marks]

Solution: Assuming a message space $\{0,1\}^n$ for some n, key-generation selects $k \leftarrow \{0,1\}^n$ uniformly at random; to encrypt $m \in \{0,1\}^n$ evaluate $c \leftarrow k \oplus m$; to decrypt $c \in \{0,1\}^n$ evaluate $m \leftarrow k \oplus c$.

Marking: One point per algorithm.

(b) Give the definition of perfect secrecy as a formal, probabilistic statement and describe in words what that statement intuitively captures.

[3 marks]

Solution: The uncertainty about a message should not decrease when seeing its ciphertext. This is formalized by requiring that, irrespective of the message distribution, for all messages m and ciphertexts c

$$\Pr[M = m | C = c] = \Pr[M = m]$$

where the lhs probability is over the choice of M and the key K.

Marking: 1 point for the intuition, 1 point for the probability statement, 1 point for a close enough quantification.

(c) There is an equivalent formalisation of perfect secrecy. Provide that statement and its intuitive meaning.

[2 marks]

Solution: The alternative is that the probability of observing a ciphertext is independent of the message, so

$$\Pr[C = c | M = m] = \Pr[C = c]$$

Marking: 1 Point for the statement, 1 point for the meaning; mixing b and c up still good for up to 4 points total.

(d) The one-time pad is seldom used directly and on its own in practice, say for secure e-mail. Why is this?

[5 marks]

Solution: There are various reasons. The one-time pad requires keys as long as the message for perfect secrecy to hold and these keys can only be used ones, creating a considerable burden on prior key arrangements. Moreover, perfect secrecy still allows malleability and provides no integrity or authenticity whatsoever. Finally, in the specific context of e-mail, a public key setting (or hybrid) makes more sense, as sender and recipient may not be known to each other (let alone have arranged some key before).

Marking: Up to 2 marks per point made, with a maximum of 5 if three or more points are made.

(e) Imagine that one would create OTP-MAC in a similar way to CBC-MAC, by encrypting a message of arbitrary length and outputting the final 128 bits (padded with zeroes if needed) as the tag. Why is this OTP-MAC a bad idea?

[2 marks]

Solution: Many reasons, for one the MAC doesn't even depend on any but the final 128 bits of the message (or key), allowing easy forgeries (by prepending message to a known message–key pair). Even worse, after seeing a single valid message–key pair (for a 128-bit message or longer), the final 128 bits of the key can be trivially recovered (and all forgeries from that point onwards are straightforward). Finally, forging a tag for a one-bit message succeeds with probability half, even without having seen any tags before.

Marking: 1 point per observation, with a maximum of 2 points.

Q3. Schnorr signatures are a way of creating signature scheme based on the discrete logarithm problem in Schnorr subgroups of $\mathbb{Z}_p^*$. Key generation and signing work as follows.

Key generation Kg Selects random 2048-bit p and 256-bit q prime numbers such that q divides $p-1$. It selects a random element $g \in \mathbb{Z}_p^*$ of order q. Let $\mathsf{G}_q \subseteq \mathbb{Z}_p^*$ be the group of order q generated by g and let $\mathsf{H} : \mathsf{G}_q \times \{0,1\}^* \to \mathbb{Z}_q$ be a hash function.

Finally, it selects a random exponent $x \in \mathbb{Z}_q$ and sets $h \leftarrow g^x \bmod p$. Publish (p, q, g, h, H) as the verification key vk and keep (p, q, g, x, H) as the private signing key sk.

Signing Sign Takes as input the private signing key $\mathsf{sk} = (p, q, g, x, \mathsf{H})$ and a message $m \in \{0,1\}^*$. It selects a random element $w \in \mathbb{Z}_q$ and sets $a \leftarrow g^w \bmod p$ followed by $c \leftarrow \mathsf{H}(a, m)$. Set $r \leftarrow w - cx \bmod q$. Return (c, r) as the signature on m.

With a suitable verification algorithm, Schnorr signatures can be proven secure—for some relevant notion of security—in the random oracle model based on the discrete logarithm problem.

(a) State the discrete logarithm problem.

[2 marks]

Solution: Given the group's description (p, q, g) and a random element h in the group, determine $x \in \mathbb{Z}_q$ such that $g^x \equiv h \bmod p$.

Marking: There is some leeway regading the DLP setting (it need not be specific to Schnorr subgroups), but the inputs, outputs, and relation $g^x = h$ need to be clear from the answer.

(b) Describe and motivate a relevant security notion for signature schemes.

[6 marks]

Solution: Various answers are possible, but good answers describe both a clear adversarial goal (e.g. selective or existential forgery) and the adversarial power (e.g. chosen message attack).

Marking: For both goal and power: typically 2 marks to describe the goal resp. power and 1 mark to motivate it.

(c) In the security reduction, what component of the signature scheme would be modelled by the random oracle?

[1 mark]

Solution: The hash function.

(d) Describe a suitable verification algorithm (hint: recompute a).

[3 marks]

Solution: Recompute a by setting $a \leftarrow g^r h^{-c}$ and accept iff $c = \mathsf{H}(a, m)$.

Marking: 2 points for the correct formula for a, 1 point for the check

For a chosen-prefix preimage attack against the hash function H, an adversary is given a target digest $z \in \mathbb{Z}_q$ and target prefix $a \in \mathsf{G}_q$, and has to find an m such that $z = \mathsf{H}(a, m)$.

(e) Prove that if H is collision resistant, then it is also resistant against chosen-prefix preimage attacks.

[4 marks]

Solution: The proof is by reduction, where we need to show how a successful adversary A against chosen-prefix preimage attacks is turned into a collision finding adversary B.

Let B create some a and m, calculate $z = \mathsf{H}(a, m)$ and feed (a, z) to A, who will return some preimage m' such that $z = \mathsf{H}(a, m')$. Then (a, m) and (a, m') form a collision, provided that $m \neq m'$. But as H is compressing, there are many possible m' for a given (h, a) and which m was chosen by B is hidden from A, so with high probability indeed $m \neq m'$.

Marking: 1 point for setting up the reduction, 1 point for B's setup, 1 point for identifying the collision, 1 point for the $m \neq m'$ argument.

(f) Show how susceptibility of H against chosen-prefix preimage attacks leads to a vulnerability against the signature scheme; name the attack against the signature scheme as precisely as possible.

[4 marks]

Solution: Suppose we are given a chosen-prefix preimage adversary A. Then we can mount a (weak) existential forgery under a known message attack. If we observe a valid message–signature pair $(m, (c, r))$, we can recompute $a \leftarrow g^r h^{-c}$ and ask A for a chosen-prefix preimage on (a, c). Then A will answer with some m' satisfying $c = \mathsf{H}(a, m')$, so $(m', (c, r))$ is a valid forgery, with $m \neq m'$ as above.

Marking: 1 point for correct naming; 3 points for the attack.

END OF PAPER