UNIVERSITY OF BRISTOL

JANUARY 2015 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 in the exam book the correct answer. Provide a short justification for each answer.

(a) The One-Time Pad is malleable.

[3 marks]

Solution: True, xoring in a known bitstring into the ciphertext will result in the same bitstring being xored into the corresponding plaintext.

Marking: For this and all other MC questions, 1 mark for the correct true/false answer (regardless of the explanation). 1 mark for the incorrect answer argued by claiming each key is used once only.

(b) CBC mode is OW-CCA secure.

[3 marks]

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

Marking: Partial marks for incorrect attack or only claiming malleability without making the attack explicit.

(c) Any probabilistic symmetric key encryption scheme is IND-CPA secure.

[3 marks]

Solution: False, the scheme $(m||r) \leftarrow \mathsf{Enc}_k(m;r)$ is probabilistic yet completely insecure.

Marking: 1 mark for proving a deterministic scheme is not IND-CPA; the mere observation that the question statement does not logically follow from IND-CPA implies probabilistic does not carry marks.

(d) A deterministic symmetric key encryption scheme cannot be OW-CCA secure.

[3 marks]

Solution: False. ECB-then-MAC is deterministic (assuming the MAC is) and gives a OW-CCA secure scheme.

Marking: 1 mark for describing an exhaustive attack on the message space. For full marks need to give explicit indication how to achieve CCA security.

(e) A homomorphic public key encryption scheme cannot be OW-CCA secure.

[3 marks]

Solution: True. If c^* is the ciphertext of unknown message m^*, create a ciphertext c for a known, non-identity element g. Use the homomorphic property to create ciphertext c' of $m^* + g$. Observe that $c' \neq c^*$, so the decryption oracle will duly return $m' = m^* + g$ on input c'. Compute m^* as $m' - g$.

Marking: Only partial marks for the observation that homomorphic implies malleable and hence cannot be CCA secure.

Q2. This question focuses on the relationship between symmetric and public key primitives.

Let $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Consider the symmetric key encryption scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ that works as follows:

Key generation Kg' runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Kg}$ and returns the pair $(\mathsf{pk}, \mathsf{sk})$ as the symmetric key k.

Encryption Enc' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a message m and returns $\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})$.

Decryption Dec' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a ciphertext c and returns $\mathsf{Dec}_{\mathsf{sk}}(c)$.

(a) Describe the IND-CCA security notion for symmetric encryption schemes.

[3 marks]

Solution: Bookwork.

Marking: One mark for the goal, one mark each for the Enc and Dec interfaces. For the goal it is important to give some meaning to the adversary's output. If m_0 and m_1 are explicitly output before oracle access, full marks are awarded (even though it is a weaker notion than what is commonly thought of as IND-CCA security).

(b) Which oracle is missing from the IND-CCA security notion of public key schemes and why?

[2 marks]

Solution: The encryption oracle is missing as it is superfluous for an adversary in possession of the public key.

Marking: One mark for naming, one mark for explanation.

(c) Prove that if the public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CCA secure, then so is the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$.

[5 marks]

(cont.)

Solution: This is a standard reduction, where the main technicality is the use of the public key to simulate the encryption queries.

To prove that if the public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CCA secure, then so is the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$. we show that if the symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CCA *insecure*, then so is the underlying public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$. Thus we are given a successful adversary A against the symmetric scheme and wish to construct a successful adversary B against the public key scheme.

The adversary B will get a public key and will then start running A. Whenever A makes an encryption query, B uses the public key to answer this query. Whenever A makes a decryption query, B uses its own decryption oracle to answer this query (directly). Once A outputs two challenge messages, B will output these challenge messages to its own game; it will return the challenge ciphertext it receives to A. Finally, once A terminates outputting a bit b', B will terminate outputting the same b'.

Marking: 2 marks for setting up the reduction (first paragraph of solution); 1 mark for IO linking (the challenge messages, ciphertext and output bit); 1 mark for forwarding dec oracle; 1 mark for using pk for enc oracle. Only providing some intuition (an adversary in the symmetric setting has less power or information than in the symmetric setting) gives up to 3 points.

(d) Show that if for some public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CCA secure, this does not imply that the original public key scheme is IND-CCA secure.

[5 marks]

Solution: Given a secure public key scheme, modify it so that the new public key consists of both the public and private key of the original scheme. This new public key scheme is trivially insecure (as the adversary is handed the private key on a plate), yet the transformation to a symmetric scheme is essentially identical to that belonging to the original scheme (which will be secure). Thus we have shown an insecure public key scheme whose related symmetric key scheme is secure, demonstrating that the implication does not hold.

Marking: For full marks, the starting point (above a secure public key scheme) needs to be clearly specified. Only describing a property of a scheme (instead of constructing one) such as 'if the private key could be recovered from the public key' drops a point. Simply stating that the lack of implication would have to be shown by counterexample (without giving one) gives 1 mark. Arguing where the reduction breaks down gives 2 marks.

Q3. This question focuses on signature schemes and the related use of hash functions.

(a) Give the generic syntax of a signature scheme (in the standard model) by describing which algorithms are involved and what their general input/output behaviour is. Also include the appropriate correctness requirement.

[4 marks]

Solution:

A *signature scheme* comprises a triple of algorithms:

Key generation Kg is a probabilistic algorithm that returns a public verification key vk and a private signing key sk.

Signing Sign is a (probabilistic) algorithm that on input a signing key sk and a message m returns a signature s.

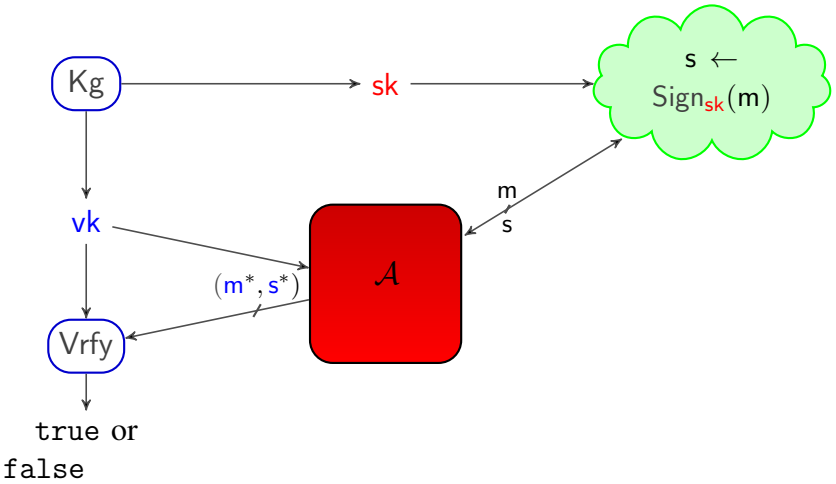
Verification Vrfy is a (deterministic) algorithm that on input a verification key vk, a message m and a purported signature s, returns either `true` (valid) or `false` (invalid).

Correctness requires that all honestly generated signatures are valid.

Marking: One point for each of the algorithms, one point for correctness requirement.

(b) Describe the security model which should be satisfied by an EUF-CMA secure scheme in the standard model by giving a diagram depicting the relevant security game together with an informal explanation (in words).

[3 marks]



Solution:

An adversary with access to the public key and a signing oracle is trying to create a

(cont.)

valid forgery $(\mathsf{m}^*, \mathsf{s}^*)$ with the restriction that m^* was not queried to signing oracle.

Marking: 1 point for formalizing what a forgery is, 1 point for getting the oracle access right, 1 point for getting the restriction on the forgery right.

Pitfalls: Providing a verification oracle instead of the verification key gives MAC notion (and would give 2 points).

(c) The hash-then-sign paradigm can be used to extend the domain of a signature scheme. Given a signature scheme with domain $\{0,1\}^n$ and an arbitrary hash function $H : \{0,1\}^{2n} \to \{0,1\}^n$, the corresponding hash-then-sign signature scheme can sign messages in $\{0,1\}^{2n}$. Describe how the hash-then-sign scheme works by specifying the relevant algorithms.

[3 marks]

Solution: Key generation stays as is, new signing by hashing the message then signing the digest, new verification by hashing (the message), then verifying the digest–signature pair.

Marking: 1 point per algorithm.

(d) Consider the hash function $H : \{0,1\}^{2n} \to \{0,1\}^n$ defined by $H(x_0||x_1) = x_0 \oplus x_1$ (that is, the input to H is split in two equal parts that are subsequently xored together). Evaluate the security of the resulting hash-then-sign scheme.

[5 marks]

Solution: The hash function is totally insecure. It is easy to find many preimages to any digest z by picking some r and setting the input to $(z \oplus r||r)$. This implies collisions and second-preimages. Collisions in the hash function lead to a EUF-CMA attack (query the signing oracle on one of the colliding message, output the resulting signature as forgery on the second colliding message). The ability to find second-preimages allows the adversary control over one of the colliding values, leading to the stronger UUF-CMA and EUF-KMA attacks regardless of the security of the underlying signature scheme. Moreover, if the underlying signature scheme itself is not EUF-CMA secure, then neither will the construction be.

Marking: Points given whenever insecurity is argued with some convincing argument, where a well explained version of collisions leading to EUF-CMA insecurity being worth 4 points. Partial marks (up to 3) for observing insecurity notions of just the hash function.

Q4. This question addresses a cryptosystem using ideas from both RSA and ElGamal.

Key generation Kg randomly generates distinct primes p', q' such that $p \leftarrow 2p' + 1$ and $q \leftarrow 2q' + 1$ are prime as well. Set $N \leftarrow pq$ and let Q_N denote the group of quadratic residues modulo N, thus $z \in Q_N$ iff $z \in \mathbb{Z}_N{}^*$ and there exists a $w \in \mathbb{Z}_N{}^*$ such that $z = w^2 \bmod N$. Pick a generator g of Q_N; both g and Q_N have order $p'q'$. Select private exponent $x \in \mathbb{Z}_q$ and compute $y \leftarrow g^x \bmod N$. The public key comprises $\mathsf{pk} = (g, y, N)$ and the private key $\mathsf{sk} = (x, p', q')$.

Encryption Enc takes as input a public key $\mathsf{pk} = (g, y, N)$ and a message $m \in Q_N$. It randomly selects $r \in \mathbb{Z}_{N^2}$ and computes $c_1 \leftarrow g^r \bmod N$ and $c_2 \leftarrow m \cdot y^r \bmod N$. The ciphertext is (c_1, c_2).

Decryption Dec takes as input a private key $\mathsf{sk} = (x, p', q')$ and a ciphertext (c_1, c_2). It computes and returns $m' \leftarrow c_2 \cdot c_1^{p'q'-x} \bmod N$.

(a) Prove correctness of the cryptosystem as described above.

[5 marks]

Solution: Follows along the line of the standard ElGamal correctness, taking into account the current group properties.

Correctness requires that $m = \mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m))$ for all m and honestly generated keys. Substitution of the scheme specifics gives the equation:

$$\begin{aligned}\mathsf{Dec}_{sk}(\mathsf{Enc}_{\mathsf{pk}}(m)) &= m \cdot y^r \cdot (g^r)^{p'q'-x} \bmod N \\ &= m \cdot g^{xr} \cdot g^{rp'q'-rx} \bmod N \\ &= m \cdot (g^{p'q'})^r \bmod N \\ &= m \bmod N\end{aligned}$$

where the last equation follows from the (given) fact that g has order $p'q'$.

Marking: 1 mark for explaining correctness, 1 mark for applying it to the specifics of the scheme, 1 mark for cancelling the xr terms in the exponent, 2 marks for the final step.

Pitfalls: One can try to prove the statement using RSA style techniques, relying instead on the Chinese Remainder Theorem and Euler's theorem. This is possible, but it requires showing that $g^{p'q'r} = 1 \bmod p$. To do this, one needs to write g as a square (which exists as $g \in Q_N$ implies $g \equiv f^2 \bmod N$ for some f and hence $g \equiv f^2 \bmod p$), so that $f^{2p'} = 1 \bmod p$ by Euler's theorem. It it not correct to claim that $g^{p'} \equiv (g^{2p'})^{2^{-1}} \equiv 1^{2^{-1}} \equiv 1 \bmod p$.

(b) Give a detailed explanation how to exploit the Chinese Remainder Theorem for efficient decryption. How could you store the private key redundantly to facilitate this speed up?

[5 marks]

(cont.)

Solution: The standard trick of CRT exponentiation. Compute $m_p \cdot c_2 \cdot c_1^{p'-x} \bmod p$ and $m_q \cdot c_2 \cdot c_1^{q'-x} \bmod q$ (where we use that c_1 will have order p' modulo p instead of $2p'$ as direct application of Euler would indicate). Reconstruct $m \cdot p \cdot (p^{-1} \bmod q) \cdot m_q + q \cdot (q^{-1} \bmod p) \cdot m_p \bmod N$ Store $-x \bmod p', -x \bmod q'$ as well as $p^{-1} \bmod q$ or $q^{-1} \bmod p$.

Marking: 1 point for explaining what values m_p and m_q have to be computed; 1 point for reducing the exponents (modulo $2p'$ is fine here as well); 1 point for giving the formula for how CRT reconstruction works in general; 1 point for applying to this context; 1 point for adding the modular inverse to the key.

(c) Using your knowledge of both the RSA and the ElGamal cryptosystems, argue about the (in)security of the RSA-ElGamal cryptosystem. Make at least one positive and one negative observation.

[5 marks]

Solution: There a number of observations that can be made. As a scheme overall, it is ElGamal in the group Q_N, so IND-CPA security relies on the DDH problem in Q_N and OW-CPA security relies on the CDH problem in Q_N. Key recovery is equivalent to DLP in Q_N. The scheme is homomorphic, thus it cannot be OW-CCA secure.

Marking: 1 point for claiming homomorphism, 1 point for the justification, 1 point for the implication. 1 point for observing probabilistic, so possibly IND-CPA. 1 point for either of the DDH, CDH, DLP links.

END OF PAPER