CS60088 Foundations of Cryptography, Spring 2014–2015

End-Semester Test

22–April–2015 CSE-107, 2:00–5:00pm Maximum marks: 60

Roll no: _____ **Name:** _____

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions.*]

1. Supply brief (one-sentence) answers to the following parts. **(2 × 8)**

(a) Under what assumption is the textbook ElGamal encryption algorithm all-or-nothing secure against passive attacks?

Solution The computational Diffie–Hellman assumption

(b) Under what assumption is the semantically secure ElGamal encryption scheme IND-CPA secure?

Solution The decisional Diffie–Hellman assumption

(c) Let $n = pq$ be a product of two (large) primes. How many quadratic residues are there in $\mathbb{Z}_n^*$?

Solution $\phi(n)/4 = (p-1)(q-1)/4$

(d) What is the quadratic residuosity assumption in connection with $n = pq$ with large primes p, q?

Solution Given an $a \in \mathbb{Z}_n^*(+1)$, it is intractable to decide whether a is a quadratic residue modulo n.

(e) For which common attack model ATK, are the notions NM-ATK and IND-ATK equivalent?

Solution CCA2

(f) What is the task of an equator in a zero-knowledge protocol?

Solution To produce a transcript statistically identical to (or computationally indistinguishable from) a transcript coming from an actual run of the protocol.

(g) What is the use of the forking lemma?

Solution To prove the CMA security of a digital-signature scheme in the random-oracle model.

(h) What roles should be played by Simon the simulator in an IND-CCA2 proof of an encryption scheme in the random-oracle model?

Solution To reply to hash queries, to decrypt indifferent and adaptive chosen ciphertexts, and to supply a challenge ciphertext.

2. Let $n = pq$ be an RSA modulus (with suitably large primes p and q), and e and d the encryption and decryption keys of a party. Let the message length be l_0, and $l_0 + l_1 + 1 = |n|$. We should have $|n| \geqslant 1024$, and $l_1 = 160$ to achieve the intended security. In order to encrypt a message $m \in \{0,1\}^{l_0}$, one first chooses a random salt $r \in_U \{0,1\}^{l_1}$, and then pads m as $\mu = 0 \,||\, m \,||\, r$. A ciphertext of m is then computed as $c \equiv \mu^e \pmod{n}$.

(a) Explain how decryption is done for this scheme. **(5)**

Solution Recover the padded message μ by RSA decryption: $\mu \equiv c^d \pmod{n}$. If the most significant bit of μ (treated as an $|n|$-bit string) is not zero, report failure. Otherwise, write $\mu = 0 \,||\, m \,||\, r$ with $|m| = l_0$ and $|r| = l_1$. Return m.

(b) Establish that this scheme is not even IND-CPA secure. **(5)**

Solution We know that if $c \equiv \mu^e \pmod{n}$ and many significant bits of μ are available, then the Fujisaki–Okamoto–Pointcheval–Stern algorithm can efficiently compute the remaining bits of μ. If $c \not\equiv \mu^e \pmod{n}$, and if many significant bits of μ are known, the above algorithm may encounter inconsistency and report failure, or return a value of μ which does not satisfy $c \equiv \mu^e \pmod{n}$. In any case, one can check easily whether a reconstructed μ is correct by checking whether $c \equiv \mu^e \pmod{n}$.

In the IND-CPA game, the adversary chooses m_0, m_1, and receives the challenge ciphertext c^* of m_b with $b \in_U \{0,1\}$ chosen by the encryption oracle. Since m_0 and m_1 are known to the adversary, he runs the Fujisaki–Okamoto–Pointcheval–Stern algorithm twice with inputs m_0, c^* and m_1, c^*. One of the computations fails, and the other (with m_b, c^* as input) recovers the salt used during encryption, and pinpoints whether m_0 or m_1 was encrypted.

3. The Goldwasser–Micali encryption scheme encrypts a message bit by bit. If the bit length of the message is l and the bit length of the modulus is k, then the ciphertext consists of lk bits. Blum and Goldwasser (Crypto 1984) propose a scheme which produces ciphertexts of size $l+k$ bits only.

Let $n = pq$ be the product of two suitably large primes each congruent to 3 modulo 4. The public key is n, whereas the private key consists of p and q.

Let $m = m_1 m_2 \ldots m_l$ be a message of bit length l, that the sender wants to encrypt. The sender first chooses $x_0 \in_U \mathbb{Z}_n^*$. (S)he then successively computes $x_i \equiv x_{i-1}^2 \pmod{n}$ for $i = 1, 2, \ldots, l+1$. Let a_i be the least significant bit of x_i, and $a = a_1 a_2 \ldots a_l$. A ciphertext for m is the pair $(m \oplus a, x_{l+1})$.

(a) Describe how a ciphertext (c, x) can be decrypted. **(5)**

Solution Since the recipient knows the factorization of n (this is the private key), (s)he can efficiently compute square roots modulo n. Each of $x_1, x_2, \ldots, x_l$ is a quadratic residue modulo n. Since $p, q \equiv 3 \pmod{4}$, every quadratic residue has exactly one square root which is again a quadratic residue. Therefore, x_{i+1} uniquely identifies x_i. Starting from $x_{l+1} = x$, the square roots $x_l, x_{l-1}, \ldots, x_1$ are computed by l square-root computations. The mask a is obtained by concatenating the least significant bits of $x_1, x_2, \ldots, x_l$. Finally, the message is recovered as $m = c \oplus a$.

(b) Prove that Blum–Goldwasser encryption is semantically secure against IND-CPA adversaries under a suitable computational assumption. **(10)**

Solution Suppose that there exists an adversary which can win the IND-CPA game against the Blum–Goldwasser cryptosystem with non-negligible advantage. The adversary takes any $m \in \{0,1\}^{l-1}$. During the IND-CPA game, the adversary chooses $m_0 = 0 \,||\, m$, and $m_1 = 1 \,||\, m$. The oracle encrypts m_b and supplies a ciphertext (c, x) of m_b. XOR-ing c with m_b reveals the bits $a_1, a_2, \ldots, a_{l+1}$. For both the ciphertexts m_0 and m_1, the bits $a_2, \ldots, a_{l+1}$ are the same. Only a_1 depends on whether m_0 or m_1 is encrypted. The ability of distinguishing m_0 from m_1 is then equivalent to distinguishing $a_1 = 0$ from $a_1 = 1$. Therefore given $a_2, \ldots, a_l$ (and x_{l+1}), the adversary can, with a non-negligible advantage, determine a_1. This indicates that the BBS generator does not pass the previous-bit test, and so is not cryptographically secure, a contradiction.

(c) Is Blum–Goldwasser encryption IND-CCA2 secure? Justify. **(5)**

Solution No. The Blum–Goldwasser encryption is XOR-malleable. If (c, r) is a ciphertext for m, then $(c \oplus m', r)$ is a ciphertext for $m \oplus m'$ for any bit string m' of the same length as m. No malleable encryption can be secure against adaptive chosen ciphertext attacks.

4. Alice wants to convince Bob that she can decrypt messages encrypted by an RSA public key (n,e). Let $d \equiv e^{-1} \pmod{\phi(n)}$ be the corresponding decryption key. Assume that both p and q are safe primes, that is, $p = 2p' + 1$ and $q = 2q' + 1$ for primes p', q'. Alice must not reveal d to Bob. Moreover, to avoid chosen-ciphertext or chosen-message attacks from Bob, Alice must not produce the decryption results directly to Bob. Alice instead uses the following protocol for the demonstration of her capability of RSA decryption (more precisely, her knowledge of d).

Commitment Alice chooses a random $s \in_U \mathbb{Z}_n$ such that s is invertible modulo $\phi(n)$. Alice sends s to Bob. (We have $\phi(n) = (p-1)(q-1) = 4p'q'$, so s must be odd and not divisible by p' or q'.)

Challenge Bob chooses a random ciphertext $C \in_U \mathbb{Z}_n^*$. Bob sends C to Alice.

Response Alice decrypts C to get $M \equiv C^d \pmod{n}$. Alice computes $t \equiv s^{-1}e \pmod{\phi(n)}$. Finally, Alice sends the response $R \equiv M^t \pmod{n}$ to Bob.

Verification Bob accepts Alice if and only if $R^s \equiv C \pmod{n}$.

(a) Deduce the completeness probability of this protocol. **(5)**

Solution We have $st \equiv e \pmod{\phi(n)}$, that is, $st = e + k\phi(n)$ for some integer k. Moreover, since $C \in \mathbb{Z}_n^*$, we have $M \in \mathbb{Z}_n^*$ too. If Alice runs the protocol as stated above, we have $R^s \equiv M^{st} \equiv M^{e+k\phi(n)} \equiv M^e (M^{\phi(n)})^k \equiv M^e \equiv C \pmod{n}$. Thus, Bob accepts Alice. That is, the completeness probability is $\varepsilon = 1$.

(b) Deduce the soundness error probability of this protocol. Assume that Alice has only polynomially bounded computational power. **(5)**

Solution C is a valid ciphertext of R with respect to the decryption key $s^{-1} \equiv td \pmod{\phi(n)}$. Alice's capability of sending the correct response is equivalent to her knowledge of s^{-1}, which in turn is equivalent to her knowledge of the factorization of n. If Alice is cheating, she does not know d (equivalently, the factorization of n). Consequently, she can send a response R which is correct with negligible probability δ.

(c) Argue that this protocol has the computational zero-knowledge property. **(5)**

Solution In an actual run of the protocol, s should be coprime to $\phi(n)$. But an equator does not know the factorization of n, and cannot compute $\phi(n)$ and enforce this condition. However, since $\phi(n) = 4p'q'$, the equator should choose an odd value for s. The chance that this s is divisible by p' or q' is overwhelmingly small. That is, the equator's choice for s is computationally indistinguishable from a choice of s made by Alice.

The equator also chooses $R \in_U \mathbb{Z}_n^*$, and computes $C \equiv R^s \pmod{n}$. The equated transcript is s, C, R.

For leftover answers and rough work

For leftover answers and rough work