Midterm Exam
Selected Topics on Security and Cryptography
May 2007

Warning:

- this exam consists of a survey and an exercise of same weight in the grade
- the survey consists of 3 series of 10 questions
- each series will be independently graded
- for each survey question there is one and only one correct answer
- any wrong answer may decrease the grade

1 Surveys

1.1 Communication Security

1. Secure encryption over infinite domain cannot be achieved because
   - ☐ the encryption cannot operate with too large messages
   - √ given a ciphertext, possible decrypted plaintexts are eventually less likely than others
   - ☐ this would require a key of infinite length
   - ☐ Shannon said so

2. A symmetric encryption scheme can be considered as a special threshold secret sharing scheme for 2 participants with a threshold of 2 because...
   - ☐ we can say that the two participants share the same key
   - ☐ the plaintext and the ciphertext can be seen as the two shares for the key
   - ☐ the key and the plaintext can be seen as the two shares for the ciphertext
   - √ the key and the ciphertext can be seen as the two shares for the plaintext

3. RC4 is...
   - ☐ a broken hash function
   - ☐ designed by Joan Daemen and Vincent Rijmen
   - √ implemented in SSL
   - ☐ a secure block cipher

4. To safely throw a die over the telephone, Alice and Bob must...
   - √ use a commitment scheme
   - ☐ use one-time pad
   - ☐ trust each other
   - ☐ throw it very hard

5. In TLS, algorithm MD5 refers to
   - ☐ a block cipher
   - ☐ a hash function
   - √ a message authentication code
   - ☐ a key establishment protocol

6. Using the keep-in-touch protocol, we can
   - ☐ break over and remain good friend
   - √ agree that a transaction terminated
   - ☐ protect the confidentiality of a discussion
   - ☐ waste the bandwidth

7. Identification Friend or Foe (IFF) attacks are...
   - ☐ ciphertext only attacks
   - √ known plaintext attacks
   - ☐ chosen plaintext attacks
   - ☐ chosen ciphertext attacks

8. In TLS, the advantage of the anonymous Diffie-Hellman is in
   - ☐ pleasing two renowned cryptographers
   - √ not over-claiming some unfounded security level
   - ☐ preventing from active attacks
   - ☐ being provably secure

9. Side channels cannot...
   - ☐ break RSA
   - ☐ break SSL
   - ☐ break DES
   - √ reveal flaws in security proofs

10. In early versions of TLS using CBC encryption, when the fragment padding were correct in a forged ciphertext, the error after decryption were...
    - ☐ `invalid_error`
    - ☐ `decryption_failed`
    - √ `bad_record_mac`
    - ☐ `buffer_overflow`

1.2 Broadcast Encryption and Traitor Tracing

1. Broadcast encryption schemes can be classified as being "stateless" or "stateful" schemes. Stateless schemes ...
   - ☐ ...assume that the receivers have a high-bandwith return path to the broadcasting center.
   - √ ...imply that the receivers are able, in case of emergency, to update parts of the secret information they store.
   - ☐ ...do not require bidirectional cable network.
   - ☐ ...have a broadcast message length which never depends on the number of revoked users.

2. An important difference between broadcast encryption schemes based on Complete-Subtree Cover (CSC) and Subset-Difference Cover (SDC) is that...
   - √ ...there is significantly less secret keys to store with CSC.
   - ☐ ...there is significantly less secret keys to store with SDC.
   - ☐ ...there is significantly more keys to store with SDC, but the keys are not required to be secret.
   - ☐ ...there is significantly less secret keys to store with CSC, and furthermore, the keys are not required to be secret.

3. The main difference between broadcast encryption schemes based on Complete-Subtree Cover (CSC) and Subset-Difference Cover (SDC) is that...
   - ☐ ...schemes based on CSC are stateless while schemes based on SDC are stateful.
   - ☐ ...schemes based on CSC are stateful while schemes based on SDC are stateless.
   - ☐ ...schemes based on CSC have bandwidth requirements not depending on the total number of receivers.
   - √ ...schemes based on SDC have bandwidth requirements not depending on the total number of receivers.

4. Broadcast encryption based on Logical Key Hierarchy ...
   - ☐ ...implies that the receivers do not need to be stateful.
   - √ ...implies that the receivers need to be stateful.
   - ☐ ...implies that the receivers need to be stateful, but not all the time.
   - ☐ ...implies that the receivers need to be stateless and stateful at the same time.

5. Broadcast encryption based on Logical Key Hierarchy ...
   - ☐ ...requires that a receiver stores as many keys as users in the system.
   - ☐ ...requires that a receiver stores only public keys.
   - ☐ ...requires that a receiver is most of the time switched off.
   - √ ...requires to store a number of keys which is logarithmic in terms of the total number of users in the system.

6. In the Boneh-Franklin traitor tracing scheme, ...
   - ☐ ...a passive adversary able to break the semantic security of that scheme can break the Computational Diffie-Hellman Assumption.
   - ☐ ...a passive adversary able to break the semantic security of that scheme cannot break the Decisional Diffie-Hellman Assumption.
   - ☐ ...an active adversary able to break the semantic security of that scheme can trivially factorize RSA moduli.
   - √ ...a passive adversary able to break the semantic security of that scheme can break the Decisional Diffie-Hellman Assumption.

7. When using the Boneh-Franklin scheme, coalitions of pirates having a size strictly larger than the maximal allowed coalition size can...
   - ☐ ...generate a single, untraceable new key able to decrypt the protected content out of their own private.
   - √ ...generate an extremely large number of untraceable, new keys able to decrypt the protected content.
   - ☐ ...generate a single new key able to decrypt the protected content out of their own private keys, but that key is traceable.
   - ☐ ...generate an extremely large number of new keys able to decrypt the protected content, but that keys are traceable.

8. We would like to implement the Boneh-Franklin scheme on a prime-order group. Let p and q be two prime numbers of respective size 1024 and 1023 bits such that $p = 2q + 1$. Furthermore, let p' and q' be two prime numbers having a respective size of 1024 and 160 bits such that $p' = Nq' + 1$ for some N. On the receiver side, it is more efficient to work...
   - ☐ ...in the multiplicative subgroup of order q in $\mathbf{Z}_p^*$ since both p and q have approximately the same size.
   - ☐ ...in the additive subgroup of order q' in $\mathbf{Z}_{p'}^*$ since the modular exponentiations are done with 864-bit exponents.
   - √ ...in the multiplicative subgroup of order q' in $\mathbf{Z}_{p'}^*$ since the modular exponentiations are done with 160-bit exponents.
   - ☐ ...directly in the multiplicative group $\mathbf{Z}_p^*$ (which has an order equal to $2q$), since it is not required to have a prime-order group to implement the Boneh- Franklin scheme.

9. In the Boneh-Franklin scheme...
   - ☐ ...the private key size depends on the total number of revoked users.
   - ☐ ...the private key size depends on the total number of users in the system.
   - √ ...the private key size depends on the tracing capabilities of the linear code.
   - ☐ ...the private key size depends on the number of users which don't collude.

10. In the Boneh-Franklin scheme...
    - ☐ ...tracing can never be performed with help of the Berlekamp algorithm.
    - √ ...tracing can be performed with help of the Berlekamp algorithm in complexity $O(n^2)$, where n is the total number of users in the system.
    - ☐ ...tracing can be performed with help of the Berlekamp algorithm in complexity $O(1)$.
    - ☐ ...tracing cannot be done on revoked users.

1.3 Provable Security and Hybrid Encryption

1. The Chor-Rivest cryptosystem is...
   - ☐ provably secure.
   - ☐ a block cipher.
   - ☐ equivalent to the knapsack problem.
   - √ broken.

2. What can we say for sure about a public-key encryption scheme provably secure in the Random Oracle model?
   - ☐ A real instantiation of the scheme is secure.
   - ☐ A real instantiation of the scheme is insecure.
   - ☐ In the proof, block ciphers are replaced by random permutations.
   - √ In the proof, hash function are replaced by random functions.

3. Which of the following security notions is the strongest one for a public-key encryption scheme?
   - ☐ One-Wayness
   - ☐ Semantic Security
   - √ CCA-Security
   - ☐ Existential Unforgeability

4. Tick the *true* assertion.
   - ☐ The Luby-Rackoff construction is based on that of the advanced encryption standard (AES).
   - ☐ The Luby-Rackoff construction builds a uniformly distributed random permutation on $2n$ bits out of three uniformly distrusted random functions on n bits.
   - √ Provided that n is large enough, it is hard to distinguish a random instance of the Luby-Rackoff construction on $2n$ bits from a uniformly distributed random function on $2n$ bits.
   - ☐ None of the above assertions is true.

5. In a proof based on a sequence of games, the Gnome technique (a.k.a. lazy sampling technique) is typically,...
   - √ a bridging step.
   - ☐ used to prove the security of a public-key encryption scheme, and never used to prove that of a digital signature scheme.
   - ☐ a transition based on a failure event.
   - ☐ used to prove the security of the ElGamal public-key encryption scheme.

6. Tick the true assertion about the FDH.
   - ☐ FDH stands for *Formal Diffie-Hellman*.
   - √ FDH is a provably secure encryption scheme.
   - ☐ FDH is provably secure in the *standard* model.
   - ☐ FDH is often based on the RSA permutation.

7. OAEP+ was introduced by
   - √ Victor Shoup
   - ☐ Mihir Bellare
   - ☐ Serge Vaudenay
   - ☐ Jean-Sébastien Coron

8. What is the reason why hybrid encryption (KEM-DEM or TagKEM-DEM) can encrypt plaintexts of arbitrary length?
   ☐ because KEM/TagKEM has infinite domain
   √ because DEM has infinite domain
   ☐ because hybrid encryption is provably secure
   ☐ because adversaries have bounded capacities

9. In the proof for TagKEM-DEM in slides, what is the reason that the difference in advantage of IND-CCA PKE adversary A_E between game 0 and game 1 equals the advantage of IND-CCA TKEM adversary A_T?
   ☐ transition based on indistinguishability: IND-CCA PKE and IND-CCA TKEM games are indistinguishable since existence of a TagKEM is implied by a PKE
   ☐ transition based on bridging step: IND-CCA PKE and IND-CCA TKEM games are equivalent since TagKEM is similar to a PKE
   ☐ transition based on failure: If A_T fails, so will A_E
   √ whether it is game 0 or game 1 depends on δ

10. Abe et al. in their TagKEM-DEM paper mention in their Section 6: Conclusions that the Cramer-Shoup based TagKEM-DEM can provide streaming feature if needed. What is the reason that makes an encryption or decryption streamable?
   ☐ both encryption and decryption can be parallelized
   √ decryption can start before entire ciphertext is received
   ☐ decryption can start even before encryption has started
   ☐ TagKEM is based on a public key

2 Exercise

Malleability implies IND-CCA Insecurity

1. In GSM, a cleartext x is first encrypted by using a pseudorandom generator G into $y = \mathsf{Enc}(x) = x \oplus G(K, \mathsf{ctr})$ given a secret key K and a frame counter ctr. The ciphertext y is sent over the radio channel. Decryption $\mathsf{Dec}(y)$ is performed with the same secret key K and a synchronized frame counter.
   (a) Give two bijective functions f and g which are different from the identity function and such that $\mathsf{Dec}(f(\mathsf{Enc}(x))) = g(x)$.
   We call this property "simple malleability"
   (b) Which security property is not achieved by this encryption?
2. We consider a public-key cryptosystem Gen/Enc/Dec.
   We assume simple malleability: we assume that one knows two bijective functions f and g which are different from the identity function and such that $\mathsf{Dec}_{K_s}(f(\mathsf{Enc}_{K_p}(x))) = g(x)$ for any x where (K_p, K_s) is generated by Gen.
   (a) Recall the definition of the IND-CCA security notion.
   (b) Prove that the cryptosystem is not IND-CCA secure.
3. We consider a public-key cryptosystem Gen/Enc/Dec. Let G by a pseudorandom generator. Let (K_p, K_s) by one public-secret key pair generated by Gen. We define a hybrid cryptosystem

   $$\mathsf{Gen}/\mathsf{HEnc}/\mathsf{HDec}$$

   such that

   $$\mathsf{HEnc}_{K_p}(x) = (\mathsf{Enc}_{K_p}(\kappa), x \oplus G(\kappa))$$

   where κ is a random value which is picked every time we must encrypt a new message. (Encryption is not deterministic.)
   (a) Explain how decryption works.
   (b) By using simple malleability, show that the proposed hybrid cryptosystem is not IND-CCA secure.
   (c) Propose a way to fix this problem by slightly changing the hybrid cryptosystem definition.