Name:	Student No:
Tutorial Group (Day):	(Time):

CS2107 Quiz (30 marks) Semester 2 AY14/15 March 20,2015

1. **[5 marks]** Suppose an encryption scheme takes 2^{20} cycles to test whether a key is correct. How many seconds does it take to try all possible 32-bit keys on a single core 4GHz Chip? (express your answer in the form 2^x).

□

2. **[5 marks]** Consider an attacker who can spoof DNS responses and send them to a victim. The attacker can also "trick" the victim to send out DNS query. However, the attacker is unable to sniff DNS query sent by the victim. Recall that in order for the victim to accept the response, the 16-bit QID must match (see Lecture 5 slide 24). Since the attacker is unable to sniff the query, the attacker would not know the value of QID. Here is a way for the attacker to work around it.

   - First, the attacker tricks the victim to send out many, say $\mathbf{2^{\textit{M}}}$, queries, where ***M*** is an integer. The "questions" asked in the queries are the same and are suggested by the attacker, but the QID's are different (the QIDs are randomly chosen and not known by the attacker).
   - The attacker then immediately sends $2^{\textit{M}}$ spoofed responses to the victim. The "answers" in the responses are the same but the QID are randomly chosen.
   - As long as there is a pair of query and response having the same QID, the attack would be successful.

   What is the smallest possible value of ***M*** such that the chance of successful attack is more than 0.5? □

3. **[5 marks]** You have intercepted 4 ciphertexts C_1, C_2, C_3, C_4 generated by a stream cipher using the same secret key. The first 4 bits of the ciphertext form the IV.

   C_1 = 0111 00000000 C_3 = 1000 00001111
   C_2 = 0111 00000011 C_4 = 1000 11111111

   Suppose the plaintext of C_1 is 01010101, and the plaintext of C_3 is 00000000.

   What is the plaintext of C_2? □

   What is the plaintext of C_4? □

4. [15 marks] Security Terminologies

The following descriptions are obtained from the Web. Fill in the blanks with the most appropriate terminologies from the following list. Some choices may appear more than once in the answer. You can either write the terminology or its number in the blank space. (Ignore grammar rules on plural forms)

Requirements:

1. Confidentiality
2. Integrity
3. Authenticity
4. Non-repudiation
5. Availability
6. Usability

Cryptography objects:

7. Initial Value (IV)
8. Pseudorandom Sequence
9. Public Key
10. Private Key
11. Signature
12. mac
13. plaintext

Cryptography notions:

14. Public Key Infrastructure
15. Public Key Cryptography
16. Symmetric Key Cryptography
17. Cryptographic Hash

Attacks:

18. Denial of Service
19. Man-in-the-middle
20. Chosen-Plaintext
21. Ciphertext-only
22. Side-channel attack
23. Skimmer
24. Phlishing

Misc:

25. Biometric scanner
26. 2FA
27. Covert Channel

i. □ means that the recipient may reasonably be certain that a message was truly created by its purported author, and has not been forged by some other party.

ii. □ means that information is intelligible only to its rightful recipients.

iii. A message has its □ protected if it is infeasible for its contents to be changed in transit without any such changes being instantly obvious to the recipient.

iv. DNSSEC does not provide □ of data; in particular, all DNSSEC responses are not encrypted.

v. The threats that surround the DNS are due in part to the lack of □ checking of the data held within the DNS and in part to other protocols that use host names as an access control mechanism. In response to this, the IETF formed a working group to add DNS Security extensions to the existing DNS protocol.

vi. □ and security is actually a field of computer science study referred to in academic studies as HCISec (human-computer interaction & security). And, as mentioned above, it’s a never-ending battle – and a tricky balance. That’s because, as one study points out, there is an inherent conflict of interest between users and system owners: The top priority for users is maximum ease of use, while the top priority for system owners is the security of their system.

vii. In cryptography, a(n) □ is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve *semantic security*, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message.

viii. Authenticated Encryption with Associated Data (AEAD) is a block cipher mode of operation which simultaneously provides □ and authenticity assurances on the data.

ix. Sometime before July 10th, the CA DigiNotar was compromised, and for several months, hundreds of thousands of users—most of whom appear to be from Iran—were subject to □ attacks on HTTPS using the fraudulent certificates from DigiNotar. This event demonstrates that the problems with the existing CA system are no longer academic, and we hope that there is enough momentum building to finally upgrade everyone to a more secure □

x. (*In this question, the answers to all the 3 blanks are the same*). A certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a(n) □. The certificate includes information about the □, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that □ to communicate with its owner.

xi. They are used in completely different contexts. In public key encryption there is the notion of □ that protects sender authenticity. On the other hand in symmetric encryption there is the notion of MAC that protects the integrity of the message with an agreed MAC key between the sender and the receiver.

xii. These □ are getting so slim that it's now virtually impossible to tell whether an machine has been hacked to harvest you card details.

xiii. □ is an example of social engineering. It seeks to acquire the victim's private information by masquerading as a trustworthy entity in an electronic communication.

xiv. A(n) □ attack is an attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms

------------- END of Quiz -------------