SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Tutorial questions for L6: Symmetric Cryptography.

QUESTION 1

Sometimes encoding is performed before encryption. When this happens, it is necessary to decrypt before decoding. A commonly used encoding scheme is known as Base64 encoding. It is used for many applications including HTTP.

a) Use an online Base64 encoding/decoding tool (there's one in Cryptool-online: http://www.cryptool-online.org/, under the 'Codings' tab) to investigate Base64 encoding of simple phrases such as
   I. *This message is encoded* or
   II. *This message has not been encrypted*.
   Record the encoded messages.
b) Decode the recorded phrase to recover your original message.
c) What do you observe about the first few characters of the encoded versions of the two messages given above?
d) Can you construct any other messages with this same characteristic?

QUESTION 2

Alice wants to send a message to Bob, without Carol (or other eavesdroppers) observing it. Alice and Bob have agreed to use a symmetric cipher. Assume key exchange has already occurred, and so Alice and Bob already share a secret key which we denote *K*. Outline the cryptographic steps that:

a) Alice must follow to encrypt the plaintext *P*.
b) Bob must follow to decrypt the ciphertext *C*.

QUESTION 3

The Caesar cipher is a well known simple symmetric cipher. Go to the Cryptool-online website: http://www.cryptool-online.org/ to try performing some encryption and decryption using the Caesar cipher. Select Ciphers, Caesar/Rot 13 from the menus to get to the Caesar cipher page. Read the information, then click on 'test it' to get to the interactive part.

a) Encrypt the **plaintext** message 'This message is encrypted' using the key K=5 (Look for the key near the bottom of the screen).
b) Decrypt the **ciphertext** message 'gwC piDm lmkzGxBml Bpm umAAiom kwzzmkBtG' using the key K=8.
c) See if you can recover the plaintext message given the ciphertext 'aopz jpwoly pz lhzF Av iylhr' without being told the key. What do you have to do?
d) Encrypt a message and send the ciphertext to a friend or classmate. What do they need to do to recover the plaintext from the ciphertext?
e) What is ROT-13, and what is it used for?

QUESTION 4

What is the main difference between *encoding* and *encryption*? Who can perform:

i. Decoding?
ii. Decryption?

QUESTION 5

Suppose that a binary additive stream cipher (such as the one time pad) has been used to encrypt an electronic funds transfer. Assuming that no other cryptographic processing is used, explain how an attacker who knows the format of the plaintext message used for the funds transfer can change the amount of the funds transfer without knowing anything about the key that is used.

QUESTION 6

Suppose that a compact disc (old fashioned, I know!) with 700MB data storage has been filled with random data to be used as keying material for the one-time pad.

a) Approximately how many email messages of 10000 characters can be perfectly secured using the disc?
b) Why is this not a useful basis for implementing secure email for most users?

QUESTION 7

Suppose that a single ciphertext bit of a received ciphertext message has been modified (changed, not deleted). When decryption is performed, how many bits in the decrypted plaintext would be expected to be in error in each of the following cases:

a) The cipher is a binary additive stream cipher;
b) The cipher is a block cipher operating in electronic codebook (ECB) mode;
c) The cipher is a block cipher operating in cipher block chaining (CBC) mode.

Suppose now that a single ciphertext bit of a received message has been deleted. What happens now in each case?

QUESTION 8

Hash functions are commonly used for checking message integrity.

a) List four basic properties of hash functions.
b) Use the internet to locate a SHA-1 demonstration tool. (There's one at http://www.movable-type.co.uk/scripts/sha1.html with explanatory text). Investigate the four basic properties by examining the SHA-1 hashes for the following messages:
    i. Take $100 from my account
    ii. Take $1000 from my account
    iii. Take $100 from your account
    iv. Investigate other hashes for both longer (at least a paragraph) and shorter messages.
c) A common application of hash functions is to produce a 'checksum', 'fingerprint' or 'message digest' of an electronic document or file. Supose you receive a document and an MD5 hash value intended as the document 'fingerprint'.
    i. How can you (the recipient) make use of the 'fingerprint', and
    ii. What assurance can be obtained from it?
d) Another application of hash functions is for password verification. User passwords should not be stored in plaintext, although many organizations still do this.
    i. Read the article 'Cupid Media Hack Exposed 42M Passwords' available at http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/. Who was affected by this breach, and how?
    ii. A better option is for organizations to store the hash values for user passwords, rather than the plaintext passwords. Explain how authentication of the user is performed in that case.

QUESTION 9
Alice wants to send a message to Bob. Alice wants Bob to be able to check that the message did not change in transit. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a MAC.

QUESTION 10
Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not change in transit and also that the contents remains confidential (protected from eavesdroppers). Explain the steps required to achieve both security goals if Alice and Bob use both a MAC and a symmetric encryption algorithm with an existing shared secret key *K*. In your answer, explain what must be done by:

a) Alice as the sender, and
b) Bob as the receiver.

QUESTION 11
In the United States of America, several states have introduced legislation requiring organisations to provide protection for personally identifying data by encrypting it. Nevada was the first state to introduce such legislation, followed by Massachusetts. Read the article at:
http://www.huntonprivacyblog.com/2009/06/articles/nevada-updates-encryption-law-and-mandates-pci-dss-compliance/

a) List the situations outlined in the article where encryption is now required.
b) Do you think Australia should introduce similar legislation? Justify your answer.