SCIENCE AND ENGINEERING FACULTY

INB255/INN255 Security

Semester 1 2014

Outline solutions for 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?

This exercise is intended to reinforce the idea that encoding and decoding are processes performed by following an algorithm - no secret key is required. A glance at the Base64 encoding of a message may not immediately reveal the message contents, but it is pretty simple to recover if you want to, so this is no substitute for encryption. Part c should emphasize the idea that the same set of characters "This message " in different messages will produce the same encoded string. Any other message that begins with "This message " will also begin with the same encoded string.

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*.

Encryption:

i. **Alice prepares the message P using appropriate coding and padding if necessary.**
ii. **Alice encrypts P using the symmetric cipher algorithm and the secret key K (and IV if used), to produce the ciphertext C, where C = E(P, K).**
iii. **Alice sends the ciphertext C to Bob.**

Decryption:

i. **Bob receives the ciphertext C.**
ii. **Bob decrypts C using the symmetric cipher algorithm and the secret key K (and IV if used), to recover P, where P = D(C, K).**
iii. **Bob removes any padding and decodes if necessary to recover the**

message.

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?

This exercise is intended to reinforce the idea that both an algorithm and a key are required for encryption (and the algorithm for Caesar cipher is really simple, so this could even be done without an online tool). Playing with the keys for a fixed message shows that the even when the message and the algorithm are the same, the ciphertext is different for different keys.
(Keeping Case sensitive and leaving space characters)

For part a) Ymnx rjxxflj nx jshwDuyji

For part b) You have decrypted the message correctly

For part c) The plaintext message is: This cipher is easy to break **(Just try all decryption keys by repeatedly clicking on the + sign under Key, down below the text boxes. Watch the ciphertext alphabet shift positions against the plaintext alphabet as you do this. Check the recovered plaintext box until you find the plaintext message. This happens when K= 7. Note that for K= 33, you’ll get the same message, but with the upper and lowercase reversed:** tHIS CIPHER IS EASY TO BREAK**.)**

Part d) They need to use the same algorithm, and the same key. Unless they can break the algorithm or brute force the key (try every possible key). That’s easy to do for Caesar cipher, but harder for many other ciphers. If you are interested, you can try some other ciphers using Cryptool – however, that activity will be outside the scope of our unit (255) and will not be examinable.

Part e) ROT-13 is a Caesar cipher where the key is 13, and for a 26 character alphabet (so not case sensitive), this means that it is it’s own inverse. So if you encrypt with K=13, and then encrypt the ciphertext with K=13, you get back to the original message (since 13 + 13 = 26 and we are using a 26 character alphabet)

QUESTION 4

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

i. Decoding?
ii. Decryption?

Hopefully answering questions 1-3 has reinforced the idea that both encryption and encoding use an algorithm, but the encryption process also requires knowledge of a secret key. So

i. Anyone who knows the algorithm can decode,
ii. Only those who know both the algorithm and the secret key can decrypt (unless you can try every key, or the algorithm is weak enough that you can break it).

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.

The part of the message in which the amount is recorded remains in the same position in the ciphertext as in the plaintext. Therefore the attacker can change the ciphertext bits in that position (bitflip) which will alter the amount transferred. In general there is no way that the attacker can know whether the alteration will increase or decrease the value of the amount.

In practice the attacker may know that the amount is likely to be small and therefore only change the digits in the high value positions.

This illustrates an important point: that even though a binary additive stream cipher provides unconditional confidentiality if the one time pad is used, it <u>does not provide message integrity</u>.

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?

A standard compact disc stores approximately 700 MB of data. Since the key length and the message length are the same for the one time pad, the number of emails of length 10K characters that can be encrypted is just the number of such emails that can be stored in the 700MB space. We can calculate this as 700000000/10000 = 70000.

If we could securely transport these compact discs to each of our potential email contacts this could be a way of securing our email. But it is not very practical since we need to know in advance who we will contact (a different CD per possible contact) and also manage which key to use and how many emails have

been sent. In other words, the key management is not practical.

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?

Bitflip error:
a) Only one received plaintext bit is wrong (see slide 33).
b) The whole block will be decrypted to a random string. On average, half of the decrypted received block will be wrong (see slide 45).
c) The whole block will be decrypted to a random string as in ECB mode. In addition, the one bit of error will be fed forward in the decryption process so that there will be a one bit error in the following decrypted block. All other blocks will be decrypted correctly (see slides 48 and 49).

Deletion error:
In all cases (for both a stream cipher and a block cipher) the output will look random for as long as synchronization is lost between encryption device and decryption device. This could continue indefinitely after one bit is lost in the ciphertext if it is treated simply as a stream of bits.

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.

a) The basic hash function properties listed in the slides are:

H1: Fixed length output for arbitrary length input

H2: One-way - given M it is easy to compute H(M), but given H(M) it is hard to find M.

H3: Collision resistant - hard to find M and M_0 so that H(M) = H(M_0)

H4: A small change in M causes a large change in H(M).

b) You should find that even though the input messages are very close, the output hash values are completely different. Note that with for any message length, both long and short, the output length is 160 bits, or 40 hexadecimal digits.

c) You can apply the same hash algorithm (MD5) to the document and see if you get the same hash value. This may give some assurance that the message has not been accidentally altered. A smart attacker who deliberately alters the message would probably recalculate the hash (since it doesn't require knowledge of a key) to suit the altered message and replace the old hash value with the new one. This means that you can't rely on the application of unkeyed hash functions to pick up intentional modifications from attackers who are aware of the limitations of dedicated hash functions.

d) The Cupid Media hack in 2013:

i. **This incident exposed personal details including the names, email addresses and passwords of 42 million customers of the online dating service Cupid Media. The information was stored in plaintext by Cupid Media, and was stolen when their security was breached. If the customers use the same password for multiple accounts, then the attackers may have access to many more resources.**

ii. **If Cupid Media stored the hash value of the password, rather than the plaintext password, authentication would be performed by:**

1. **User sends UserID and password**
2. **Server computes hash value of received password**
3. **Look up record for that UserID,**
    a. **Compare computed hash value with stored hash value**
    b. **If they match, access is permitted**

This approach has the advantage that the user passwords are not stored or known to anyone at Cupid Media. To find out the password, the attackers have to compute hashes for lots of different inputs and try to find one that matches.

If the passwords were randomly chosen this would be difficult. But most attackers know the common passwords that users choose, so in practice they just hash these common passwords and look for matches with those hashes. In the Krebs article, it gives a list of the ten most commonly chosen passwords and states that more than 10% of the Cupid users had selected one of these (there were 42 million accounts, remember, so that's a lot of people using those ten passwords). This approach still has limitations – where the passwords are the same, the hash values will be also. Using salted hashes, where the salt is a random number and different for every user, is a better option but not one we

have discussed in this unit.

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.

Alice
i) Generates message M
ii) Generates MAC = H_K(M) from M using the hash algorithm H and key K
iii) Sends the pair {M, MAC} to Bob

Bob
i) Receives {M, MAC}
ii) Generates MAC_0 from M.
iii) Compares the calculated MAC_0 and the received MAC
iv) If MAC = MAC_0 then is assured message is unchanged in transit

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.

There are various ways this can be done, but not all have the same properties.

Option 1:
Alice can calculate the *MAC for the plaintext* message M first, and then encrypt the whole message and MAC together.
In this case, Bob needs to decrypt the received ciphertext first to obtain the message and MAC from Alice, and then calculate the MAC for the decrypted message and compare with the received decrypted MAC.

Option 2:
Alice can encrypt the message, then calculate the *MAC for the ciphertext* and forward the ciphertext and it's MAC to Bob.
In this case, Bob can calculate the MAC for the ciphertext he receives, and compare it with the MAC received from Alice. If they are the same, then he assumes the ciphertext is unaltered, so he can decrypt and recover the plaintext.

Advantage for Option 2: Of course, if the MACs are not the same, there is no need for Bob to put in the work required to decrypt, since he will disregard the message!

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.

The law requires the use of encryption for all records containing personal information if the information is outside the secure control of the business

- **On data storage devices moved outside of the area physically controlled by the business**
- **For personal information being transmitted across insecure networks (such as the Internet or wireless networks),**
- **For payment card information, have to comply with the Payment Card Industry Data Security Standard**

This is an interesting discussion point: how specific should legislation be, especially with respect to the use of technology?

- **If the legislation requires encryption for transmissions, is the requirement satisfied by using a Caesar cipher to encrypt? Even though this doesn't really provide a great deal of security?**
- **Do algorithms and key sizes need to be specified – but what happens if these algorithms are subsequently broken? Or improvements in technology make the key size inadequate (thinking of the 54 bit DES keys that were once considered secure)?**

Does Australia require legislation to ensure that organizations actually implement cryptographic control measures?