University of Oslo
INF3510 Information Security
Spring 2014
Workshop Questions & Answers

Lecture 5: Cryptography

Question 1

In which situations and for which purposes can cryptography be used to protect information?

Answer

Cryptography can be used to protect information when transmitted through unprotected networks or stored in places lacking physical or logical access control. Cryptography can provide confidentiality, integrity and authenticity (including non-repudiation)

Question 5

The 4 security services i) “data confidentiality”, ii) “data integrity”, iii) “data authentication” and iv) “non-repudiation of origin” are related in the sense that one service often implies/provides another. Indicate for each service which of the 3 other services is/are also provided.

Answer

i. Message confidentiality implies message integrity. In case it is assumed that the message is encrypted with a secret key known only to the sender and recipient, then it also implies message authentication.
ii. Message integrity implies message authentication when it is assumed that the Mac (Message Authenticiation Code) is generated by a secret key known only to the sender and recipient. Under that assumption, message integrity and message authentication are equivalent. Message integrity implies non-repudiation of origin when it is assumed that the DigSig is generated by a private key known only to the sender. Under that assumption, message integrity and non-repudiation of sender are equivalent.
iii. Message authentication implies message integrity.
iv. Non-repudiation of message origin implies message authentication and message integrity.

Implies→ **Service↓**	Confidentiality	Integrity	Authentication	Non-repudiation
Confidentiality	Y	Y	Y (secret key)	
Integrity		Y	Y (secret key)	Y (private key)
Authentication		Y	Y	
Non-repudiation		Y	Y	Y

Question 2

Alice wants to send a message to Bob, without Eve observing it. Alice and Bob have agreed to use a symmetric cipher. Key exchange has already occurred, and so they share a key K. Outline the steps that Alice and Bob must follow when they encrypt and decrypt, respectively.

Answer

Encryption:
i) Alice prepares the message *M*.
ii) Alice encrypts the message using the symmetric cipher algorithm in encryption mode E with the key *K*, to produce the ciphertext *C*, where $C = E(M,K)$.
iii) Alice transmits the ciphertext message to Bob.

Decryption:
i) Bob receives the ciphertext *C*.
ii) Bob decrypts the ciphertext using the symmetric cipher algorithm in decryption mode D with the key *K*, to recover *M*, where $M = D(C,K)$.
iii) Alice reads/interprets the message.

Question 3

Alice wants to send a message *M* with a digital signature Sig(*M*) to Bob. Alice and Bob have an authentic copy of each other's public keys, and have agreed on using a specific hash function h and an asymmetric algorithm which can operate in signature mode S (equivalent to Decryption mode D) or in verification mode V (equivalent to Encryption mode E). Outline the steps that Alice must follow when signing *M*, and the steps that recipient Bob must follow for verifying and validating the signature Sig(*M*).

Answer

Digital signature generation by Alice:

i. Alice prepares message *M*.
ii. Alice applies the secure hash algorithm *h* to produce hash value h(*M*).
iii. Alice uses her private key $K_{priv}(A)$ with the asymmetric algorithm in signature mode S to produce signature $Sig(M) = S(h(M), K_{priv}(A))$.
iv. Alice transmits message *M* and signature Sig(*M*) to Bob, together with her unique name and specification of the hash algorithm and the asymmetric algorithm she used.

Digital signature validation by Bob:

i. Bob receives message *M'* (denoted as *M'*, not *M*, because its origin is uncertain), as well as the signature Sig(*M*).
ii. Bob applies the secure hash algorithm h on *M'* to produce hash value h(*M'*).
iii. Bob recovers hash h(*M*) from signature Sig(*M*) by using Alice's public key $K_{pub}(A)$ with the asymmetric algorithm in verify mode V to produce $h(M) = V(Sig(M), K_{pub}(A))$.
iv. Bob checks that h(*M*) = h(*M'*). If TRUE, then the signature Sig(*M*) is valid, meaning that *M'* = *M*. Bob therefore is convinced that Alice sent message *M'*. If FALSE, then the signature Sig(*M*) is invalid, meaning that $M' \neq M$. Bob therefore does not know who created the received message *M'*. He might then decide to reject the message, or use it knowing that its origin is uncertain.

Note:
The reason why Bob − and in fact anybody who knows Alice's public key $K_{pub}(A)$ − can be convinced that Alice sent message *M* is that only Alice could have produced the corresponding digital signature Sig(*M*) because it is assumed that only she knows and possesses the private key $K_{priv}(A)$. The semantic interpretation of the digital signature is still not totally clear. It could e.g. mean

a) Alice sent the message but doesn't necessarily agree with its content
b) Alice agrees with the content of the message.

In the paper-and-pen world, interpretation (b) is normally assumed. In the digital communications world, interpretation (a) is normally assumed.

Question 4

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, show that an attacker can change the amount of the funds transfer without knowing anything about the key used. (You may assume that the attacker knows the format of the plaintext message used for the funds transfer.)

Answer

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 bits in that position 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 that a binary stream cipher provides no message integrity even though it can provide unconditional confidentiality if the one time pad is used.

Question 5

Hash functions are commonly used for checking message integrity.

a. List the four basic requirements of cryptographic hash functions
b. What's the difference between the two variants of collision resistance ?
c. Use the internet to locate an SHA-1 demonstration tool — there's an interactive one written by Eugene Styer that can be used at http://people.eku.edu/styere/Encrypt/JS-SHA1.html. Investigate the four 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 and shorter messages

Answer

a. The four basic hash function properties are:
b. H1: Easy to compute h(*M*).
   H1: Fixed length output for arbitrary length input
   H2: One-way - given h(*M*), it is computationally impossible to find message *M*
   H3: Collision resistant – computationally impossible to find *M* and *M'* so that h(*M*) = h(*M'*)
c. Weak: Given one specific *M,* hard to find *M'*. Strong: Pick any *M*, hard to find *M'*.
d. 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.

Question 6

a. What is the meaning of the term MAC ?
b. What is the difference between a MAC and a hash function?
c. In what ways can a hash value be secured so as to provide message authentication?
d. Imagine that a specific hash function is used for HMAC, and that vulnerabilities have been found in the hash functions so that the HMAC is insecure. Which changes in the HMAC are required in order to make it secure again?

Answer

a. MAC can mean two things:
   1) the algorithm for the keyed hash function, or
   2) the result output of the keyed hash function.
b. A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC algorithm, by definition, uses a secret key to calculate an integrity check code (MAC) which provides data authentication.
c. Hash codes can be secured to become a MAC in various ways: HMAC, CBC-MAC and CMAC are examples
d. To replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module.

Question 7

Alice wants to send a message to Bob. Alice wants Bob to be able to verify that the message has not changed in transit. For this they use a MAC function with a shared secret key *K* for generating and verifying a MAC value denoted Mac. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying the Mac.

Answer

Alice:
i) Generates message *M*
ii) Generates Mac = MAC(*M,K*) with *M* and *K* as input parameters
iii) Sends {*M,* Mac} to Bob

Bob
i) Receives {*M',* Mac} (message denoted as *M'* because its integrity is uncertain)
ii) Generates Mac′ = MAC(*M',K*) from *M'* and *K*.
iii) Compares Mac′ and Mac
iv) If Mac = Mac′ then Bob knows the message has not changed in transit

Question 8

a. Explain why message authentication alone is insufficient as proof of message origin in general, and to settle disputes about whether messages have been sent.
b. What security service is provided by digital signatures, and explain how this service relates to message authentication.
c. In what order should the signature function and the encryption function be applied? Also explain why that order makes sense.
d. How can a sender give a plausible reason for repudiating a signed message?

Answer

a. Suppose that John sends an authenticated message to Mary. The following disputes that could arise: 1. Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share. 2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.
b. Digital signatures provide non-repudiation, which is stronger than authentication because it provides proof to third parties of message origin.
c. It is important to perform the signature function first and then an outer confidentiality function. In case of dispute, some third party must view the message and its signature. If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message. However, if the signature is the inner operation, then the recipient can store the plaintext message and its signature for later use in dispute resolution.
d. The sender can claim that the private signature key was stolen.

Question 9

The Diffie-Hellman key agreement algorithm achieves key agreement by allowing two hosts to create a shared secret.

a. Clearly explain the operation of the Diffie–Hellman key exchange protocol.
b. Clearly explain why the basic Diffie–Hellman protocol does not provide any assurance regarding which other party the protocol is run with.

Answer

a. They share a base g and a modulo m. Let a and b be the secret keys of A and B respectively. Then:
   • A → B : g^a (mod m)
   • B → B : g^b (mod m)
   • *A* computes $(g^b)^a = g^{ab}$ (mod m)
   • *B* computes $(g^a)^b = g^{ab}$ (mod m)
   A,B now share the symmetric key g^{ab}

b. The basic Diffie-Hellman protocol includes no authentication of the messages exchanged. Therefore Alice has no assurance that she is running the protocol with Bob and Bob has no assurance that he is running the protocol with Alice.