

Name ID Section Seat No

Sirindhorn International Institute of Technology Thammasat University

Final Exam: Semester 2, 2011

Course Title: CSS322 Security and Cryptography

Instructor: Steven Gordon

Date/Time: Wednesday 4 April 2012; 9:00–12:00

Instructions:

- This examination paper has 21 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).

Question 1 [7 marks]

The original standard for encryption in a wireless LAN (WiFi) is called Wired Equivalent Privacy (WEP). Early devices that used WEP allowed the user to select a 10 hexadecimal digit value, which was combined with a 24-bit initialisation vector to produce the encryption key. The IV was sent as plaintext and changed for every packet sent.

- (a) What is the entropy of the user selected value? [1 mark]
- (b) An alternative to entering a hexadecimal value would be to allow the user to enter the key using the 94 ASCII printable characters. How many characters are needed for the ASCII-based key? [2 marks]

When a user can select an ASCII string (from the 94 printable characters) they normally do not choose it randomly. One study has calculated the approximate entropy of ASCII strings if the user can choose: any value; any value, except for those in a dictionary. The entropy values for different length strings is shown in Table 1.

Table 1: Entropy of user chosen ASCII strings

<i>Length</i>	<i>Any Value</i>	<i>Any Value, except Dict.</i>
6	14	23
10	21	32
14	27	36
18	33	40
20	36	42
22	38	44
24	40	46
30	46	52
40	56	62

An improved security protocol for wireless LAN is called WiFi Protected Access (WPA). It allows a 256-bit key, generated from a password chosen by the user of between 8 to 63 printable ASCII characters. Assume a malicious user can attempt to guess the password at a rate of 1,000 guesses per second.

(c) If the user chose a 10 character password and was allowed any value, on average approximately how long would it take the malicious user to guess the password? [2 marks]

(d) If the user is allowed to choose a password with any value, except that from a dictionary, then what is the minimum password length that offers the same strength as the 10 hexadecimal digit value in part (a)? [2 marks]

Question 2 [8 marks]

The following shows the partial output of the `/etc/shadow` file on a Linux operating system. This file store the usernames and password related information for users of the computer. The values are separated by a `:` character. (Note that the data for each user is normally on a single line; I have wrapped it across two lines to fit within the page for this question).

```
boonsita:$5$8MlKVqhP$sdF897ds12poheds9032.asjfeiojfsdf9REWk32ds/
```

```
chavalit:$6$8jWr21do$0rx85gh9Tz3C5k9sTwoKOVWmFwteaLmR.TkzIdNFCdc1NfqNI
362apshyCIKFE8yBxkBhwMJ1ABCLGQ7N4t6H/
```

```
tossapong:$1$KWas931B$89jASDI3fs.kjlds9FP01/
```

A portion of the `crypt` man page is shown below. It describes the format of the second field from the `/etc/shadow` file above.

If `salt` is a character string starting with the characters `"id"` followed by a string terminated by `"$"`:

```
$id$salt$encrypted
```

then instead of using the DES machine, `id` identifies the encryption method used and this then determines how the rest of the password string is interpreted. The following values of `id` are supported:

ID	Method
1	MD5
2a	Blowfish (not in mainline glibc; added in some Linux distributions)
5	SHA-256 (since glibc 2.7)
6	SHA-512 (since glibc 2.7)

So `5salt$encrypted` is an SHA-256 encoded password and `6salt$encrypted` is an SHA-512 encoded one.

"salt" stands for the up to 16 characters following `"id"` in the salt. The encrypted part of the password string is the actual computed password. The size of this string is fixed:

MD5	22 characters
SHA-256	43 characters
SHA-512	86 characters

The characters in "salt" and "encrypted" are drawn from the set `[azAZ09./]`.

Answer the questions based on the information above. Assume the users chose their passwords randomly. Assume the algorithms used have no flaws.

(a) Can you tell which user has the longest password? Explain your answer. [2 marks]

(b) Assuming Tossapong chose a password p , then write an equation showing how the “encrypted” value, e , is calculated. Use the names of any algorithms and specific values from the file in the equation. [2 marks]

Concentrating on user Boonsita, assume the Linux system has forced her to choose a 6-character password. A malicious user has paid for database of 10^9 6-character passwords and their corresponding MD5 hash values. The database has no compression or efficient data structures.

(c) How much data is stored in the database? [2 marks]

(d) Can the malicious user use the database to try to find Boonsita’s password? If yes, explain how. If no, explain why not. [2 marks]

Question 4 [5 marks]

Listing 1 shows a set of packets captured when using SSH (further packets were captured beyond frame 38; they are not shown). Listing 2 shows details for selected individual packets from Listing 1. For clarity, some information that is not necessary for answering questions has been removed. Also, some values have been changed to make calculating answers easier.

Listing 1: SSH Packet List

No.	Time	Source	Dest.	Proto	Info
16	0.133487	1.1.1.1	2.2.2.2	SSHv2	Server Protocol: SSH-2.0-OpenSSH_4.7p1 Debian-8
18	0.133642	2.2.2.2	1.1.1.1	SSHv2	Client Protocol: SSH-2.0-OpenSSH_5.3p1 Debian-3
20	0.158486	2.2.2.2	1.1.1.1	SSHv2	Client: Key Exchange Init
21	0.159471	1.1.1.1	2.2.2.2	SSHv2	Server: Key Exchange Init
24	0.212451	2.2.2.2	1.1.1.1	SSHv2	Client: Diffie-Hellman GEX Request
26	0.235424	1.1.1.1	2.2.2.2	SSHv2	Server: Diffie-Hellman Key Exchange Reply
28	0.238691	2.2.2.2	1.1.1.1	SSHv2	Client: Diffie-Hellman GEX Init
29	0.283398	1.1.1.1	2.2.2.2	SSHv2	Server: Diffie-Hellman GEX Reply
31	0.321912	2.2.2.2	1.1.1.1	SSHv2	Client: New Keys
33	0.369375	2.2.2.2	1.1.1.1	SSHv2	Encrypted request packet len=48
35	0.382345	1.1.1.1	2.2.2.2	SSHv2	Encrypted response packet len=48
37	0.819498	2.2.2.2	1.1.1.1	SSHv2	Encrypted request packet len=64
38	0.850053	1.1.1.1	2.2.2.2	SSHv2	Encrypted response packet len=64
...					

Listing 2: SSH Packet Details

Frame 20 (858 bytes on wire, 858 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 788

Padding Length: 8

Key Exchange

Msg code: Key Exchange Init (20)

Algorithms

kex_algorithms string: diffie-hellman-group-exchange-sha256

server_host_key_algorithms string: ssh-rsa

encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr

encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr

mac_algorithms_client_to_server string: hmac-md5,hmac-sha1

mac_algorithms_server_to_client string: hmac-md5,hmac-sha1

compression_algorithms_client_to_server string: none

compression_algorithms_server_to_client string: none

KEX First Packet Follows: 0

Frame 21 (850 bytes on wire, 850 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 780

Padding Length: 10

Key Exchange

Msg code: Key Exchange Init (20)

Algorithms

kex_algorithms string: diffie-hellman-group-exchange-sha256

server_host_key_algorithms string: ssh-rsa

encryption_algorithms_client_to_server string: aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr

encryption_algorithms_server_to_client string: aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr

mac_algorithms_client_to_server string: hmac-md5,hmac-sha1

mac_algorithms_server_to_client string: hmac-md5,hmac-sha1

compression_algorithms_client_to_server string: none

compression_algorithms_server_to_client string: none

KEX First Packet Follows: 0

Frame 24 (90 bytes on wire, 90 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 20

Padding Length: 6

Key Exchange

Msg code: Diffie-Hellman GEX Request (34)

DH GEX Min: 00000008

DH GEX Numbers of Bits: 00000008

DH GEX Max: 0000000F

Frame 26 (218 bytes on wire, 218 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 148

Padding Length: 8

Key Exchange

Msg code: Diffie-Hellman Key Exchange Reply (31)

Multi Precision Integer Length: 129 (decimal)

DH modulus: 239 (decimal)

Multi Precision Integer Length: 1 (decimal)

DH base: 7 (decimal)

Frame 28 (210 bytes on wire, 210 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 140

Padding Length: 6

Key Exchange

Msg code: Diffie-Hellman GEX Init (32)

Multi Precision Integer Length: 128 (decimal)

DH client e: 184 (decimal)

Frame 29 (786 bytes on wire, 786 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 700

Padding Length: 9

Key Exchange

Msg code: Diffie-Hellman GEX Reply (33)

KEX DH host key length: 277 (decimal)

KEX DH host key: 000000077373682D727361000000012300000101009C5052...

Multi Precision Integer Length: 129 (decimal)

DH server f: 122 (decimal)

KEX DH H signature length: 271 (decimal)

KEX DH H signature: 000000077373682D72736100000100172CEA9394795589C5...

MAC: 000000C0A15000000000000000000000

Frame 31 (82 bytes on wire, 82 bytes captured)

SSH Protocol

SSH Version 2

Packet Length: 12

Padding Length: 10

Key Exchange

Msg code: New Keys (21)

Frame 33 (114 bytes on wire, 114 bytes captured)

SSH Protocol

SSH Version 2

Encrypted Packet: 4F8BD30EB384B2AB713CA1785F17CBF17410E9F4DD82783C...

MAC: 1751A0F06C0C13EB2C4478C4

Frame 35 (114 bytes on wire, 114 bytes captured)

SSH Protocol

SSH Version 2

Encrypted Packet: 912DAFF5E864321439AA2454496AC4D5539E350BE7F3833D...

MAC: BFD7C9EDEB3926E3CB36E29B

- (a) What block cipher mode of operation is used in Frame 33? [1 mark]

- (b) What is the key length used in the encryption in Frame 33? [1 mark]

- (c) What MAC algorithm is used in Frame 33? [1 mark]

In SSH the client authenticates the server based on the public key of the server (which is assumed to be known by the client).

- (f) After receiving which frame can the client authenticate the server in the above SSH connection? Explain why you selected the frame. [2 marks]

Question 5 [5 marks]

Consider the X.509 certificate in Listing 3.

Listing 3: X.509 Certificate

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3 (0x3)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=TH, ST=Pathumthani, O=ThammasatUniversity, OU=SIIT,
           CN=SIITTU/emailAddress=security@siit.tu.ac.th
    Validity
      Not Before: Jan 25 02:25:10 2011 GMT
      Not After : Jan 25 02:25:10 2013 GMT
    Subject: C=TH, ST=Pathumthani, O=AIT, OU=ComputerScience,
           CN=CSAIT Security/emailAddress=security@cs.ait.ac.th
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        1f:aa:1f:cf:01:2f:d3:2e:80:63:98:1b:0f:16:5d:
        dd:af:e2:38:de:78:88:56:b6:14:2b:61:79:92:0b:
        f3:7f:b6:89:7b:d0:fc:59:5a:1a:be:24:61:39:d5:
        4d:80:3a:40:2b:7c:89:ef:5e:50:a5:3b:44:68:a9:
        7f:97:d9:c4:9a:bf:b6:97:eb:4c:87:0d:00:96:b4:
        f9:ea:8c:6a:cb:e0:bd:f8:a8:1f:82:d3:2b:23:3c:
        b6:54:85:37:5b:13:1a:2e:be:0d:20:52:c5:98:b6:
        4c:97:67:6e:b2:43:04:3f:01:41:8e:e0:2f:38:1f:
        e1:cc:cf:0d:c2:5f:0a:04:da
      Exponent: 3 (0x3)

    Signature:
      a5:7a:36:91:ef:11:46:58:74:37:87:81:7a:99:ff:b6:40:4a:
      80:6a:07:69:e3:3c:33:9a:fd:31:50:e9:9f:bf:ff:36:a4:34:
      21:50:49:70:e0:88:b3:01:c9:51:26:8b:1e:8b:34:ca:4c:3c:
      a2:ab:0a:a3:b3:39:c0:fb:88:72:98:69:c9:af:42:b2:48:1b:
      4e:4a:76:e8:b4:c7:d4:f8:15:d2:5e:f8:69:fc:53:0c:ca:85:
      84:ea:e5:36:17:20:65:fc:d0:3e:d1:33:17:f7:d1:40:f8:3d:
      2a:87:f8:3c:66:8e:43:62:ea:02:ef:7a:d4:a7:55:e9:d9:2d:
      38:1a
-----BEGIN CERTIFICATE-----
MIIC5zCCA1CgAwIBAgIBAzANBgkqhkiG9w0BAQUFADCBnzELMAkGA1UEBhMCVEgX
GDASBgNVBAGTC1BhdGh1bXRoYW5pMREwDwYDVQQHEWhCYW5na2FkaTENMAzGA1UE
ChMEU01JVDEMMGA1UECzMDSUNUMR4wHAYDVQQDEExVDXZJJoawZpY2F0ZSBBdXRo
b3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NzczMyMi1jYUBpY3Quc2lpdC50dS5hYy50
aDAeFw0xMTAxMjUwMjI1MTBhFw0xMjUwMjI1MTBhMFYxCzAJBgNVBAYTA1RI
MRQwEgYDVQQIEwtQYXRodW10aGFuaTENMAzGA1UEChMEU01JVDEMMGA1UECzM
SUNUMR4wHAYDVQQDEwEZW1vIFVzZXIgmjCBnzANBgkqhkiG9w0BAQEFAA0BjQAw
gYkCgYEAqh/PAS/TLoBjmBsPFL3dr+I43niIVrYUK2F5kgvzf7aJe9D8wVoaviRh
OdVNgDpAK3yJ715QpTtEaKl/19nEmr+2l+tMhw0AlrT56oxqy+C9+KgfgtMrIzy2
VIU3WxMaLr4NIFLfmLZM12duskMEPwFBjuAvOB/hzM8Nw18KBKCAwEAAa7MHkw
CQYDVROTBAlwADAsBg1ghkgBhvCAQOEHxYdt3B1b1NTTCBHZW51cmF0ZWQgQ2Vy
dG1maWnhdGUwHQYDVROBBYEF0oc3MUW8p28YV6o0mcqBhPFZiQuMB8GA1UdIwQY
MBaAFGFSQOp/40x3QfZPb3xJ6wXBVm1JMA0GCSqGSIb3DQEBBQUAA4GBAKV6NpHv
EUZYdDeHgXqZ/7ZASoBqB2njPDOa/TFQ6Z//zakNCFQSDgiLMBYVEmix6LNMpM
PKKrCqQz0cD7iHKYacmvQrJIG05Kdui0x9T4FdJe+Gn8UwzKhYtq5TYXIGX80D7R
Mxf30UD4PSqH+DxmjkNi6gLvetSnVenZLTga
-----END CERTIFICATE-----
```

- (a) Whose certificate is this? [1 mark]
- (b) Whose key is used to create the signature? [1 mark]
- (c) Assume your computer received the above certificate. To verify the certificate your computer (or an application on it) performs the following test:

```
if condition then 'verified'  
else 'error'
```

Write a statement for `condition` (e.g. `A==B`). In your statement you must use the names of algorithms and values from the above certificate (i.e. you cannot use `E()`), as well as clearly identify owners of keys. Use the field names from the certificate in your statement. [3 marks]

Question 6 [10 marks]

Consider the mechanism illustrated in Figure 1.

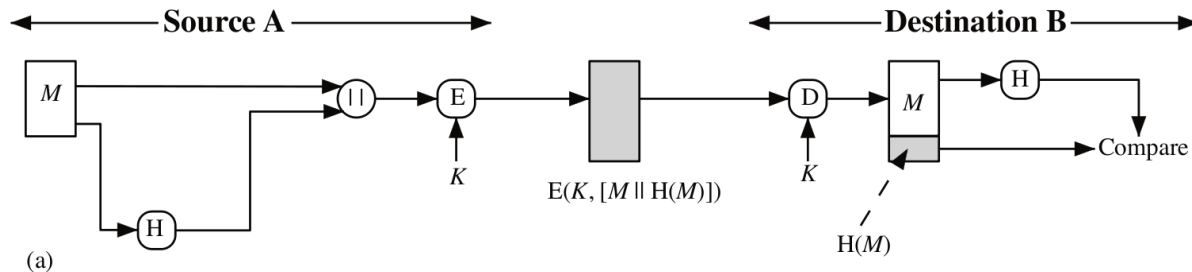


Figure 1: Security mechanism 1

- (a) List all security services provided by this mechanism. [2 marks]

- (b) Explain (or define) the *weak collision resistant property* (also called *second pre-image resistant property*) of a hash function. [2 marks]

- (c) If the function $H()$ does not satisfy the weak collision resistant property, then explain what an attacker can attempt to do to defeat the above security service. [3 marks]

- (d) Explain (or define) the *strong collision resistant property* (also called *collision resistant property*) of a hash function. [2 marks]
- (e) Which property is easier for an attacker to defeat: weak collision resistant or strong collision resistant? [1 mark]

Question 7 [5 marks]

Your web browser has just accessed `https://it.siit.tu.ac.th/moodle`. Your computer is using an Ethernet LAN card.

- (a) Draw a protocol stack that shows the specific protocols that the data from your web browser passes via. [2 marks]

Your web browser has established a secure session and connection to a web server. The browser stores the following information about the session/connection.

- Session ID: id
- Compression method: null
- CipherSuite: TLS_DH_RSA_WITH_AES_CTR_MD5
- Master secret: m
- Server MAC secret: x_s
- Client MAC secret: x_c
- Server random: y_s
- Client random: y_c
- Server encrypt key: z_s
- Client encrypt key: z_c

Figure 2 shows the general operation of the SSL record protocol.

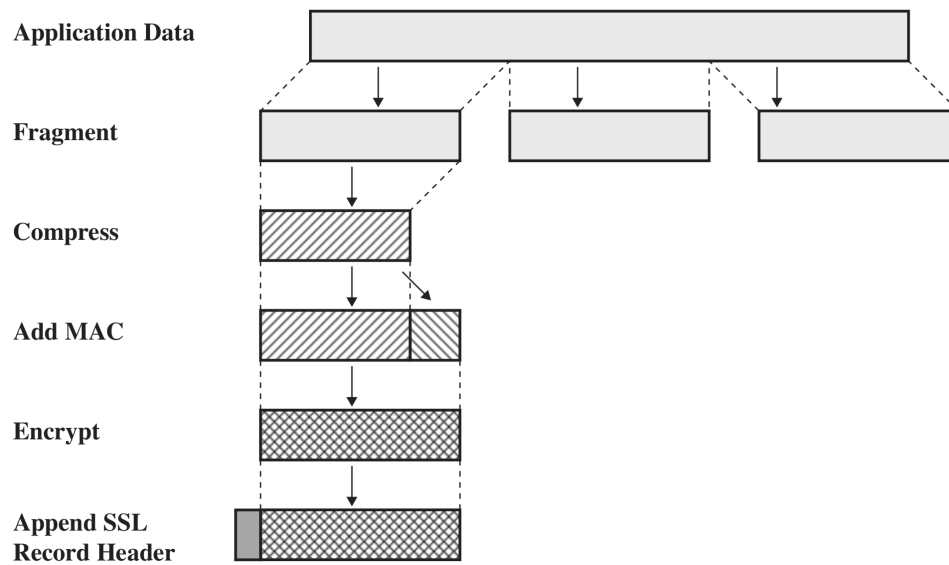


Figure 2: SSL Record Protocol Operation

- (b) Write an equation that expresses the SSL record operation on a single data fragment, D , from the web server that produces the packet to be sent P . Use the variables above and $||$ for the concatenate/append operator. For function names you *must* use the algorithm names (i.e. you cannot use $E()$ for encrypt, $H()$ for hash; refer to specific algorithms). Denote the SSL header as S . [3 marks]

Question 8 [9 marks]

(a) Draw a diagram that illustrates a reflector DDoS attack. Show (and label) the nodes involved and the direction of messages. [2 marks]

(b) Of the nodes involved in the reflector attack above, which nodes are controlled (or infected) by the malicious user? [1 mark]

(c) What are two advantages of a reflector DDoS attack compared to a direct DDoS attack? [2 marks]

Question 9 [6 marks]

- (a) User A wants to send a MAC authenticated message M to B . Give an equation that describes what is sent to B , i.e. $Sent = \dots$. You must also describe all variables used. [2 marks]
- (b) Assume a malicious user C intercepts the message sent by A . C modifies the message M . Can B detect this modification? Explain your answer (i.e. what B does to detect or why B cannot detect). [2 marks]
- (c) Explain why MAC-based authentication cannot be used as a digital signature. [2 marks]

Question 10 [12 marks]

Consider the key distribution protocol illustrated in Figure 3.

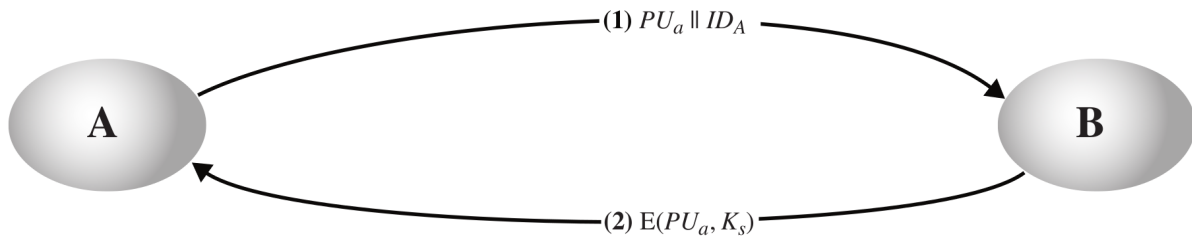


Figure 3: Key distribution 1

- (a) What key is this protocol trying to distribute? [1 mark]
- (b) Draw a diagram that illustrates how a malicious user C can perform a man-in-the-middle attack. Clearly label all messages sent. [3 marks]

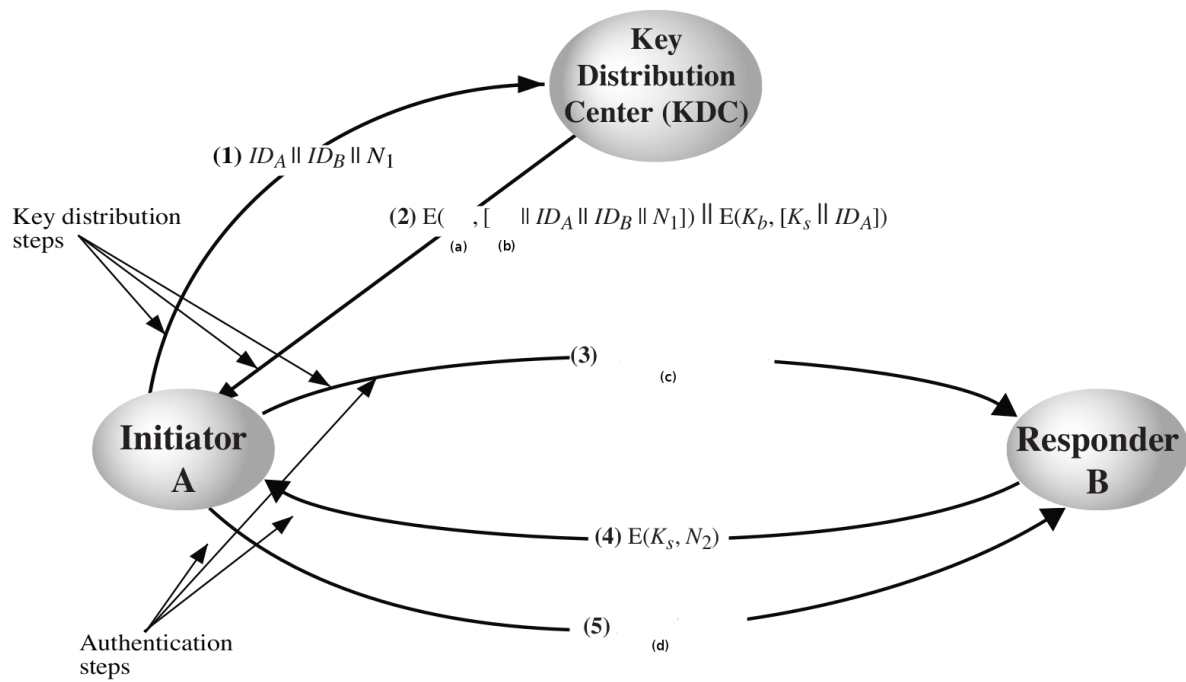


Figure 4: Key distribution 2

Consider the key distribution protocol illustrated in Figure 4. There are four missing values in the figure. What are they?

(c) [1 mark]

(d) [1 mark]

(e) [1 mark]

(f) [1 mark]

Assume there are 1000 users in a network using the key distribution protocol of Figure 4.

(g) What is the maximum number of master keys in the network at any one time? [1 mark]

(h) What is the maximum number of session keys in the network at any one time? [1 mark]

(i) What is the advantage of using both master and session keys (compared to just using master keys)? [2 marks]