课堂练习三：RSA

程宇帅

22131069@zju.edu.cn

13588212894

Problem 1:

Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:

P = 11, q = 13, e = 11; M = 45

Answer

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

$$n = p \times q = 11 \times 13 = 143$$

$$\Phi(n) = (p-1)(q-1) = 10 \times 12 = 120$$

$$d \equiv e^{-1}\left(mod\ \Phi(n)\right) = 11^{-1} mod\ 120 = 11$$

$$\therefore C = M^e\ mod\ n = 45^{11}\ mod\ 143 = 89$$

Problem 2:

In a public-key system using RSA algorithm, you intercept the ciphertext C = 67 sent to a user whose public key is e = 11, n = 91. What is the plaintext M ?

Answer

Key Generation by Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p - 1)(q - 1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

$$n = p \times q = 91 = 7 \times 13$$

$$\Phi(n) = (p-1)(q-1) = 6 \times 12 = 72$$

$$d \equiv e^{-1}\left(mod\ \Phi(n)\right) = 11^{-1} mod\ 72 = 59$$

$$\therefore M = C^d\ mod\ n = 67^{59}\ mod\ 91 = 72$$

课堂练习四：ElGamal

程宇帅
22131069@zju.edu.cn
13588212894

Problem

用户Alice和Bob执行Elgamal加密方案，其中q=157，α=5.

（1）如果用户Bob的公开钥Y_B=10，Alice选择随机整数k=5，明文M=9对应的密文是什么？

（2）如果用户Alice选择了另一个k值，明文M=9的密文为C=（25，C_2），请问C_2是什么？

Answer

（1）$1 \le M = 9 \le q-1,\ \ 1 \le k = 5 \le q-1$

$K = (Y_B)^k \bmod q = 10^5 \bmod 157 = 148$

将M加密成明文对(C_1, C_2)，其中

$C_1 = \alpha^k \bmod q = 5^5 \bmod 157 = 142$

$C_2 = KM \bmod q = 148 \times 9 \bmod 157 = 76$

$C = (C_1, C_2) = (142, 76)$

（2）$1 \le M = 9 \le q-1$

$C_1 = \alpha^k \bmod q = 5^k \bmod 157 = 25$

$\therefore\ \ k = 2$

$K = (Y_B)^k \bmod q = 10^2 \bmod 157 = 100$

$C_2 = KM \bmod q = 100 \times 9 \bmod 157 = 115$

课堂练习五：Key Distribution

程宇帅

22131069@zju.edu.cn

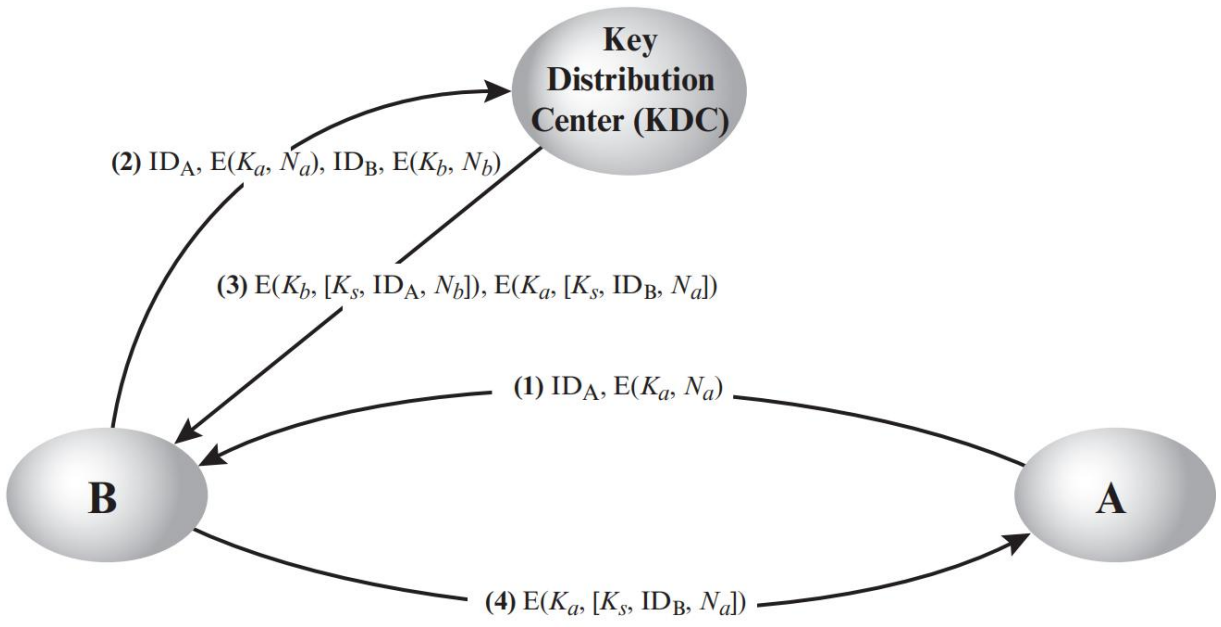
13588212894

Problem

14.1 One local area network vendor provides a key distribution facility, as illustrated in Figure 14.17.

a. Describe the scheme. 描述密钥分配方案

b. Compare this scheme to that of Figure 14.3. What are the pros and cons? 优缺点



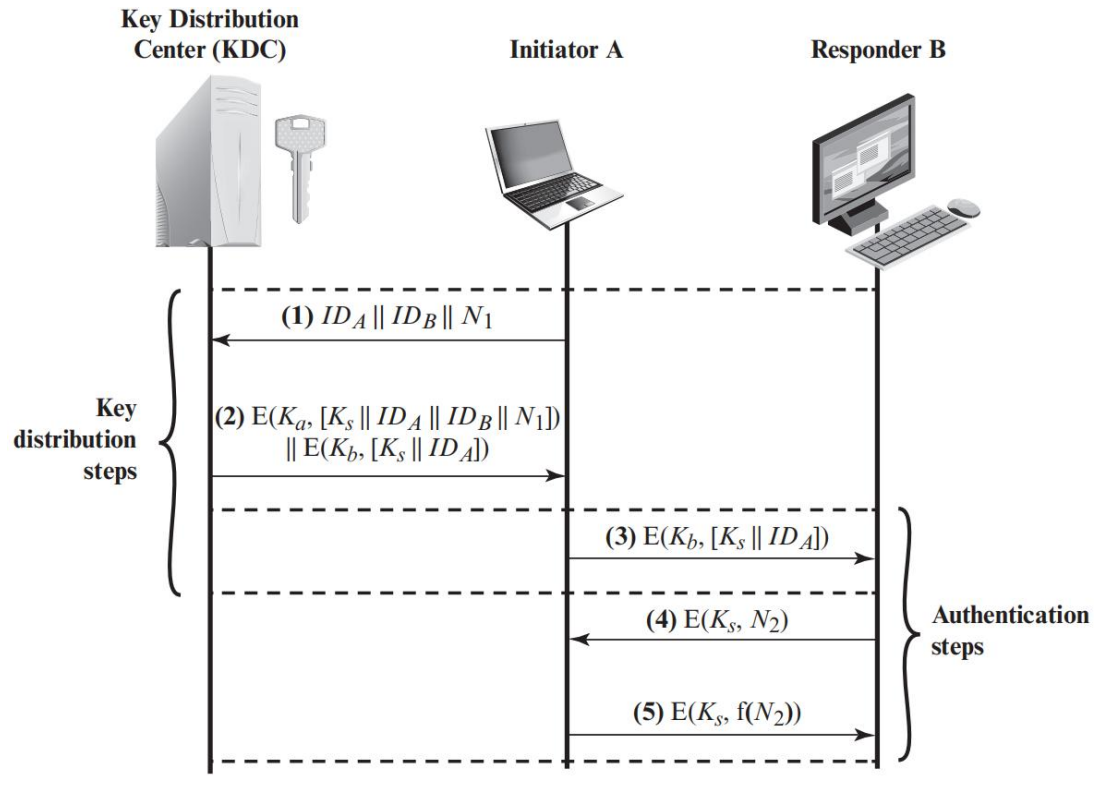


Figure 14.3 Key Distribution Scenario

Answer

a.（1）A发起连接请求，给B发送A的标识符ID_A以及用A的主密钥K_a（只有A和KDC知道）加密的唯一标识N_a。N_a为临时交互号（nonce），临时交互号可以是时间戳、计数器或者随机数。

（2）如果B准备接受连接，它将向KDC发送一个会话密钥的请求，内容包括A的标识符ID_A，由A产生并用K_a加密的唯一标识N_a，B的标识符ID_B，由B产生并用K_b加密的唯一标识N_b。

（3）KDC发送加密消息给用户B，消息由两部分组成，一部分的接收者是用户B，内容用B的主密钥K_b（只有B和KDC知道）加密，包括会话密钥K_s，A的标识符ID_A和N_b。另一部分的接收者是用户A，内容用A的主密钥K_a加密，包括会话密钥K_s，B的标识符ID_B和N_a。

（4）B将为A准备的消息内容传递给A。由于该部分包含了由A产生并用K_a加密的唯一标识N_a，因此A和B都可以安全地获得会话密钥。

Answer

b. 可以从开销角度（消息交互次数），抗攻击角度（重放攻击）和功能实现（身份认证）等方面加以分析。

首先，总体上看14.17的消息交互有4步，14.3有5步，但就密钥分配来说，14.17的密钥分配步骤为4步，14.3的密钥分配步骤为前3步，而14.3的步骤（3）到步骤（5）实现的是认证功能，这个认证功能是14.17所没有的。

第二，从抗重放攻击角度看，14.17的步骤（1）无法抗重放攻击，步骤（2）和步骤（3）可以抗重放攻击，14.3的步骤（1）至步骤（5）均可抗重放攻击。

因此，总的来说，与14.3相比，14.17的优点是：消息数变少，14.3需要交互5次，14.17只需要交互4次，因此减小了开销；缺点是：14.17中没有身份认证步骤，而14.3中的步骤（3）至步骤（5）执行了认证功能；14.17步骤（1）无法抗重放攻击，14.3中每一步都可以抗重放攻击。

课堂练习一：Playfair 加解密

程宇帅

22131069@zju.edu.cn

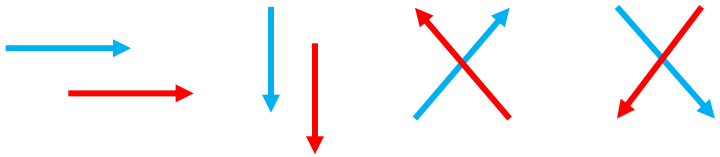
13588212894

1.(a) 请用密钥security建playfair矩阵，并加密消息See you at New Bridge Gate. Please come here at once.

解：（1）建立playfair矩阵（将密钥去掉重复字母后，按从左到右，从上到下的顺序填入5×5的表格，剩下的字母按顺序填，j和i占同一个空格，或者不填j）

S	E	C	U	R
I/J	T	Y	A	B
D	F	G	H	K
L	M	N	O	P
Q	V	W	X	Z

（3）加密过程：



蓝色为明文，红色为密文。

（2）加密规则：

① 若明文对为连续重复字母，则在重复字母中间插入“X”；

② 若明文是奇数个字母，则在最后补上“X”；（先①后②）

③ 若两个字母在同一行，则用右边的字母分别代替（最右边的列则用左边第一列代替）；

④ 若两个字母在同一列，则用下面的字母分别代替（最下面的行则用最上面的行代替）；

⑤ 对角线上的字母则用反对角线的字母分别代替。

（4）加密结果

明文：SE EY OU AT NE WB RI DG EG AT EP LE
AS EC OM EH ER EA TO NC EX

密文：EC CT XA BY MC ZY SB FH CF BY RM MS
IU CU PN UF CS UT AM WY UV

(b) 请用密钥communication建playfair矩阵，并解密消息FBCLDOEIKIBW！

解：（1）建立playfair矩阵

C	O	M	U	N
I/J	A	T	B	D
E	F	G	H	K
L	P	Q	R	S
V	W	X	Y	Z

（2）按加密的逆过程解密

明文：FB CL DO EI KI BW

密文：HA VE AN IC ED AY

消息为： HAVE A NICE DAY！

课堂练习二：AES

程宇帅
22131069@zju.edu.cn
13588212894

Problem:

Given the plaintext {00010203040506070809 0A0B0C0D0E0F} and key {10101010101010101010101010101010}:

(a) Show the original contexts of STATE, displayed as a 4×4 matrix;

(b) Show the value of STATE after initial AddRoundKey;

(c) Show the value of STATE after SubBytes;

(d) Show the value of STATE after ShiftRows;

(e) Show the value of STATE after ColMix.

Answer:

（a）矩阵将明文按列排序。

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

（b）轮密钥加，明文与密钥按位异或。

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

$\oplus$

10	10	10	10
10	10	10	10
10	10	10	10
10	10	10	10

$=$

10	14	18	1C
11	15	19	1D
12	16	1A	1E
13	17	1B	1F

（c）字节代换，将字节的高4位作为行值，低4位作为列值，以行列值为索引从S盒（参考资料P_{181}）的对应位置取出元素作为输出。

x \ *y*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

CA	FA	AD	9C
82	59	D4	A4
C9	47	A2	72
7D	F0	AF	C0

（d）行移位，状态的第一行保持不变，第二行循环左移一个字节，第三行循环左移两个字节，第四行循环左移三个字节。

CA	FA	AD	9C
82	59	D4	A4
C9	47	A2	72
7D	F0	AF	C0

→

CA	FA	AD	9C
59	D4	A4	82
A2	72	C9	47
C0	7D	F0	AF

（d）列混淆，矩阵乘法运算，乘积矩阵中的每个元素均是一行和一列中的对应元素的乘积之和。其中，乘法和加法都是定义在GF（2^8）上的。

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

×

CA	FA	AD	9C
59	D4	A4	82
A2	72	C9	47
C0	7D	F0	AF

=

06	87	8F	56
45	A2	4E	E5
97	4D	8B	7A
25	49	7A	3F

以第一个元素为列，（{02}·{CA}）⊕ （{03}·{59}）⊕ （{01}·{A2}）⊕ （{01}·{C0}）= {06}

1.在网络或 internet 上，和用户认证关联的三个威胁

1.用户可以获得对特定工作站的访问，并假装是从该工作站操作的另一用户。2.用户可以改变工作站的网络地址，使得从改变的工作站发送的请求看起来来自模拟的工作站。3.用户可能会窃听交易所并使用重放攻击来进入服务器或扰乱操作。

2.消息认证和用户认证的区别和联系

区别：

1、性质不同

身份认证指通过一定的手段，完成对用户身份的确认。

消息认证（message authentication）指验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。它包含两层含义：验证信息的发送者是真正的而不是冒充的，即数据起源认证；验证信息在传送过程中未被篡改、重放或延迟等。

2、目的不同

身份验证的目的为确认当前所声称为某种身份的用户，确实是所声称的用户。在日常生活中，身份验证并不罕见；比如，通过检查对方的证件，我们一般可以确信对方的身份。虽然日常生活中的这种确认对方身份的做法也属于广义的“身份验证”，但“身份验证”一词更多地被用在计算机、通信等领域。

消息认证目的为了防止传输和存储的消息被有意无意的篡改。

3.

15.10 In Kerberos, when Bob receives a Ticket from Alice, how does he know it is genuine?
15.11 In Kerberos, when Bob receives a Ticket from Alice, how does he know it came from Alice?

如何知道受到的票据是真实的？

如何知道票据来自 alice？

15.10 It contains the Alice's ID, Bob's name, and timestamp encrypted by the KDC-Bob secret key.

15.11 It contains Alice's name encrypted by the KDC-Bob secret key.

- 包括 alice 的 id，bob 的名字和由 KDC Bob 密钥加密的时间戳
- 它包含由 KDC Bob 密钥加密的 Alice 的名字。

4.消息认证码和数字签名的区别

Mac 跟数字签名也有很多区别和联系的。

Mac 跟数字签名也有类似的地方，因为都可以确认发出人身份，同时判断文件有无被篡改。

但是区别也是明显的，因为生成 Mac 和验证 Mac 需要的密钥是同一个，属于对称加密的范畴。而数字签名属于非对称加密，生成签名用私钥，而验证签名是否有效要用公钥。Mac 的工作方式决定了，发送方和接收方要事先共享同一个密钥，这也是对称加密算法的共性。数字签名的接收方是不能再生成签名的，也就是说不可伪造。但是 Mac 的接收方因为手里也有密钥，所以可以对其他信息生成 Mac 。