白文强 20191060064

第二章 课后作业

1、这个问题是现实世界中一个对称密码的例子，它来自于以前美国的特种部队手册。这个文件的文件名为 Special Foreces.pdf，可以在 box.com/CompSec3e 网站上获得。

a. 利用两个密钥（内存字）cryptographic 和 network security，加密下面的文字：Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.

对于怎样处理内存字中冗余字母和过多字符以及怎样处理空白和标点符号进行合理的假设。说明你的假设是什么。

将冗余字母删除，将多余字符保留第一个，空白字符和标点符号忽略。

将两个秘钥分别按照顺序排列，同时去除重复字母，根据字母出现的顺序转换为对应的数字 1 至 10，将第一次转换得到的密文再用第二个密钥转换一次，最后输出密文。

加密：

第一次加密

2	8	10	7	9	6	3	1	4	5
C	R	Y	P	T	O	G	A	H	I

加密过程：

将明文依次按行写入下表：

B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

第二次加密：

4	2	8	10	5	6	3	7	1	9
N	E	T	W	O	R	K	S	C	U

在第一次加密的表中，按照数字顺序，依次取出一列，在第二次加密中按行排列。

T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D
I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

再次根据数字顺序，依次取出一列，顺序排列，即为加密后的密文：

ISRNG BUTLF RRAFR LIDLP FTIYO NVSEE TBEHI HTETA EYHAT TUCME HRGTA IOENT TUSRU IEADR FOETO LHMET NTEDS IFWRO HUTEL EITDS

b. 对密文进行解密，并给出解密结果。

这两个矩阵的使用顺序是相反的。首先，密文在第二个矩阵中以列的形式排列，根据第二个秘钥对应的数字表示的顺序填写矩阵：

4	2	8	10	5	6	3	7	1	9
T	R	F	H	E	H	F	T	I	N
B	R	O	U	Y	R	T	U	S	T
E	A	E	T	H	G	I	S	R	E
H	F	T	E	A	T	Y	R	N	D

I	R	O	L	T	A	O	U	G	S
H	L	L	E	T	I	N	I	B	I
T	I	H	I	U	O	V	E	U	F
E	D	M	T	C	E	S	A	T	W
T	L	E	D	M	N	E	D	L	R
A	P	T	S	E	T	E	R	F	O

按行取出矩阵中的内容，进行第一次解密。将第一次解密后的内容根据第一个秘钥对应的数字表示的按列填写矩阵：

2	8	10	7	9	6	3	1	4	5
B	E	A	T	T	H	E	T	H	I
R	D	P	I	L	L	A	R	F	R
O	M	T	H	E	L	E	F	T	O
U	T	S	I	D	E	T	H	E	L
Y	C	E	U	M	T	H	E	A	T
R	E	T	O	N	I	G	H	T	A
T	S	E	V	E	N	I	F	Y	O
U	A	R	E	D	I	S	T	R	U
S	T	F	U	L	B	R	I	N	G
T	W	O	F	R	I	E	N	D	S

最后，从左到右、从上到下读取矩阵的内容，即为解密后的明文：

BE AT THE THIRDPILLAR FROM THE LEFT OUT SIDE THE LYCEUM THEATRE TO NIGHTAT SEVEN IF YOU ARE DISTRUSTFUL BRING TWO FRIENDS

c. 讨论在什么时候适合采用这项技术，以及它的优点是什么。

在发送时间敏感信息的时候适合采用这项技术，即使密文被敌方收到，暴力破解密码也需要 10^10 * 10^10 次，破译之后，该密文的时效性也过了。

该技术的优点在于运算简单方便，并且由于采用了两个秘钥，可以很好地预

防中间相遇攻击，较大程度上保证信息安全。

2、考虑一个非常简单的对称分组加密算法，利用一个 128 位的密钥对 64 位明文分组进行加密。加密过程定义如下：$C=(P\oplus K_0)\boxplus K_1$

这里 C=密文；K=秘密密钥；K0=K 的最左边的 64 位；K1=K 的最右边的 64 位，$\oplus$=按异或操作；$\boxplus$是模2^{64}加法运算。

a. 写出解密方程，也就是将 P 表示为 C、K1 和 K2 的函数。

解密方程：

P = $(C-K1+2^{64})\%2^{64}\oplus$ K0

b. 假设攻击者已经获得了两套明文和对应的密文并希望确定密钥 K，有两个方程：

$C=(P\oplus K_0)\boxplus K_1;\ C'=(P'\oplus K_0)\boxplus K_1$

首先推导出只含有一个未知量（如 K0）的方程。是否可以进一步求出 K0？

可以进一步求得 K0。由于已推导出只含有一个未知量(如 K0)的方程，说明已求出 K1，只需要将 1 组明文和对应密文即可以代入解密方程，即可求出 K0。

3、比较一下由数字签名（DS）和消息认证码（MAC）提供的安全服务。假定 Oscar 可以看到 Alice 发给 Bob 的所有信息，也可以看到 Bob 发给 Alice 的所有消息，对于数字签名，Oscar 除了公钥之外不知道其他任何密钥。解释：（i）DS 和（ii）MAC 是否能防御下面各种攻击以及如何防御。auth(x)的值分别用 DS 和 MAC 算法计算。

a. （消息完整性）Alice 将消息 x=“将 1000 美元转账给 Mark”以明文的形式发送给 Bob，并连同 auth(x)一起发给 Bob。Oscar 中途截获了该消息并用“Oscar”替换“Mark”。那么 Bob 可以检测出来吗？

都可以检测出来：

若采用 DS 提供的安全服务，对消息 x 进行散列，并将散列的结果和 Alice 的

私钥采用数字签名生成算法形成数字签名并将数字签名拼接在消息后面，Bob 收到消息后，会将明文消息 x 进行散列，并将散列结果、Alice 的公钥以及拼接在消息 x 后的数字签名放入数字签名认证算法进行认证。由于消息 x 被修改了，数字签名验证失败，则 Bob 能检测出来消息被修改。

若采用 MAC 算法，将消息 x 和 Alice 和 Bob 的共同秘密秘钥 K 生成 MAC，并将 MAC 附在消息 x 后，Bob 收到消息后，会取出明文生成 MAC，与发送来的 MAC 进行比较，Oscar 修改了消息 x，则生成的 MAC 与原 MAC 不同，则 Bob 就检测出了消息被修改。

b.（重放）Alice 将消息 x="将 1000 美元转账给 Oscar"以明文的形式发送给 Bob，并连同 auth(x)一起发给 Bob。Oscar 观察到了该消息和签名，并将其发送给 Bob100 次。那么 Bob 可以检测出来吗？

采用数字签名：

可以检测出来，若 Alice 对数组签名报文添加了时间戳，那么 Oscar 将拦截到的消息和签名发送给 Bob，Bob 会对报文的时间戳进行验证，若出现重复的时间戳，则说明遭受到了重放攻击

采用 MAC:

不可以检测出来，由于双方共同秘密秘钥是不变的，那么对同一个消息产生的认证信息是一样的，不会发生改变，那么 Bob 将持续接收 100 次该报文，无法检测出重放攻击。

c.（欺骗第三方的发送方认证）Oscar 声称他将消息 x 连同有效的 auth(x)发送给了 Bob。而 Alice 却说是她发的。那么 Bob 可以区分出是谁发的吗？

采用数字签名：

可以区分出来，数字签名由消息以及发送者的私钥进行加密，Oscar 没有 Alice 的私钥，所以 Bob 可以通过用 Alice 的公钥以及接收到的消息进行数字签名的认证区分出是否是 Alice 发送的消息。

采用 MAC：

不可以区分，若 auth(x)是有效的，那么，只能说明发送者拥有与 Bob 的共同秘密秘钥，但是若 Bob 与 Alice 之间共同秘密秘钥被 Oscar 窃取，则 Bob 收到的消息可能来自于 Oscar，也可能来自 Alice。

d. （Bob 欺骗认证）Bob 声称他从 Alice 那里收到了 x 消息和有效的签名 auth(x)（如“将 1000 美元从 Alice 那里转账到 Bob”），但是 Alice 说她没发过这样的消息。那么 Alice 能解释清楚这个问题吗？

采用数字签名：

无法解释清楚。由于数字签名具有签名可信性、不可抵赖性、不可复制性、不可伪造性，因此，如果 Bob 收到的 auth(x)是有效的，那么 Alice 无法抵赖。

采用 MAC：

可以解释，由于 MAC 采用双方共同秘密秘钥以及消息生成，Bob 也有该秘钥，完全可能是 Bob 可以给自己发消息并声称是 Alice 发的， Alice 可以通过此进行解释。