网络安全与检测技术 作业 1

提交截止时间：11 月 10 日（周日）23:59:59

1. AES-CBS-STAR

令 E_k 和 D_k 分别为 AES 分组密码中的加密和解密算法。

(1) 我们设计一种新的分组密码工作模式 AES-CBS-STAR。一个消息 M 被分为明文分组 $M_1, \ldots, M_n$，每个明文分组为 128 比特。加密过程如下

$$C_0 = \text{IV}(\textbf{generated randomly})$$
$$C_i = E_k(C_{i-1} \oplus M_i) \oplus C_{i-1}$$

请写出解密 M_i 的表达式（由 AES 解密算法 D_k 和相应密文分组得到 M_i 的方式）。

(2) 请分析该工作模式有可能对多个明文分组进行并行加密吗？解密呢？

(3) 我们再设计一个 AES-CBS-STAR 的修改版，AES-CBS-SHARP。假设 IV 不再是随机生成的，而是从一个给定的随机数集合中进行选择，这个集合是公开的，对手（the adversary）知道这个集合中的随机数。如果用 IV_i 作为加密对手的第 i 条信息的 IV。请尝试说明对手能够赢得 IND-CPA 游戏。

2. 分组加密模式的错误传播

(1) 在 ECB 模式中，密文模块 8 的比特 17 在传输过程中被污染了。请找出原文可能被污染的比特。

(2) 在 CTR 模式中，密文模块 2 和 3 被完全污染了。请找出原文可能被污染的比特。

(3) 在 OFB 模式中，密文模块 7 整个被污染了（$s = 8$）。请找出原文可能被污染的比特。

(4) 在 CBC 模式中，密文模块 9 的比特 16 和 17 在传输过程中被污染了。请找出原文可能被污染的比特。

(5) 在 CFB 模式中，密文模块 12 的比特 3 到 6 在传输过程中被污染了。请找出原文可能被污染的比特。

3. RSA

考虑下列方法：

S1: 挑选一个奇数 E。

S2: 挑选两个素数 P 和 Q，其中 $(P-1)(Q-1)-1$ 是 E 的偶数倍。

S3: P 和 Q 相乘得 N。

S4: 计算

$$D = \frac{(P-1)(Q-1)(E-1)+1}{E}.$$

这种方法是否与 RSA 等价？请说明原因。

4. Hash

利用加密算法构造单向 Hash 函数。考虑使用又一个已知密钥的 RSA 算法。如下处理含有若干分组的消息：加密第一分组，将加密结果与第二分组异或并加密之，等等。

通过解决下面问题，说明该方法是不安全的。给定两个分组消息 B1, B2，其 Hash 码为

$$\mathrm{RSAH}(B1, B2) = \mathrm{RSA}(\mathrm{RSA}(B1) \oplus B2)$$

给定任一分组 C1，选择 C2 使得 $\mathrm{RSAH}(C1, C2) = \mathrm{RSAH}(B1, B2)$。因此该 Hash 函数不满足抗弱碰撞性。

5. MAC 验证

在 Keyczar 密码库的一个早期实现中，有以下验证 MAC 的函数（已简化）：

```
def verify(key, msg, sig_bytes):
    return HMAC(key, msg) == sig_bytes
```

其中，“==”是基于逐字节比较实现的，当第一个不相等的字节出现时，即返回 false。假设存在一个攻击者，希望利用这个性质来构造针对目标消息 m 的 MAC 标签，请问这个攻击如何实施？你能否改写上述 verify 函数，避免此类攻击？

6. 机密性和完整性

Alice 和 Bob 想要其通讯具有机密性和完整性（confidentiality and integrity）。有以下工具供他们使用

- 对称加密
  - 加密：$\mathsf{Enc}(K, m)$
  - 解密：$\mathsf{Dec}(K, c)$
- 密码散列函数：$\mathsf{Hash}(m)$
- 消息认证码：$\mathsf{MAC}(K, m)$
- RSA 签名

- 签名：$\mathsf{Sign}(SK, m)$
- 验证：$\mathsf{Verify}(PK, m, sig)$

他们之间共享一个对称密钥 K，并且他们知晓彼此的公钥。Alice 有以下几种方式给 Bob 发送消息：

(a) $c = \mathsf{Hash}(\mathsf{Enc}(K, m))$

(b) $c = c_1, c_2 : c_1 = \mathsf{Enc}(K, m), c_2 = \mathsf{Hash}(\mathsf{Enc}(K, m))$

(c) $c = c_1, c_2 : c_1 = \mathsf{Enc}(K, m), c_2 = \mathsf{MAC}(K, m)$

(d) $c = c_1, c_2 : c_1 = \mathsf{Enc}(K, m), c_2 = \mathsf{MAC}(K, \mathsf{Enc}(K, m))$

(e) $c = \mathsf{Sign}(SK_A, \mathsf{Enc}(K, m))$

(f) $c = c_1, c_2 : c_1 = \mathsf{Enc}(K, m), c_2 = \mathsf{Enc}(K, \mathsf{Sign}(SK_A, m))$

请回答以下问题：

(1) 以上哪几种方式 Bob 可以解密密文 c 获得明文 m?

(2) 假设存在一个窃听者 Eve，她可以看到 Alice 和 Bob 之间通讯的密文 c。在（1）的答案中，哪几种方式可以提供机密性保护?

(3) 假设存在一个中间人 Mallory，他可以偷听并且修改 Alice 和 Bob 之间的通讯。在（1）的答案中，哪几种方式可以提供完整性保护?

(4) 上面的几种方式都无法抵御重放攻击（replay attack）。如果 Alice 和 Bob 之间需要发送多条消息，攻击者 Mallory 可以记录之前发送过的某条消息，并在后面某个时间将其发送给 Bob，从而欺骗 Bob 使其以为这条消息来自 Alice。在上述四种方式中，选择一种可以同时保护机密性和完整性的方式作为基础，并将其修改为可以抵御重放攻击的方式。

7. "Why so serious?"

这一题无标准答案，需要你自行进行调研，选择一种合理的情形进行作答即可。

(1) 假设你想要实施一个攻击，针对基于人脸识别的门禁系统。请思考一种可能的攻击角度，并描述其威胁模型。

(2) 假设你想要设计一个安全的文件分享系统。请列出你设计的系统想要的安全性质，并描述其威胁模型。

8. 附加题

见 Lec05 Hash&MAC 第 55 页。