Homework 1 (Information Security)

Swapnil Hasabe

sdh140430

Q1. Symmetric Encryption

Secret Key: 00112233445566778899887766554

Initialization Vector(IV): 123124122

I used following command to decrypt Test1.b. Output is in decrypt_test1.txt

openssl enc -d -aes-128-cbc -iv 123124122 -K 00112233445566778899887766554 -in Test1.b -out decrypt_test1.txt

Output in file- “Hello World!”

Q2.Hash Function 10%

openssl sha1 Test1.b SHA1(Test1.b)= ebe29446ad8d413d275f2da20879560936ff2183

Q3.Message Authentication Codes (MAC) 10%

***Is SHA-1 vulnerable to “length-extension attacks”?**

Ans : Yes, SHA-1 vulnerable to “length-extension attacks”

***If we use SHA-1 as a hash function, is H(K || message) a secure message authentication code?**

Explain.

Ans: H (K||message) is not secure message authentication code because it is vulnerable to “length –extension attacks”.

Suppose,

1)H is the hash function original message M and secret key K i.e. H(K||M).

2) Now attacker will use “length- extension attack” in which attacker will do padding to massage M. It means he will add extra bits M1 to massage M to form:

M’= M+M1.

3) Then calculate its hash H’= H (H (K||M)||M1)

4) (Collision Concept) On receiving, Receiver will not able to identify difference between H and H’. The receiver will get altered message. Here, hash of previous message block as input is used to construct new hash of next block.

***Is SHA-3 vulnerable to “length-extension attacks”?**

Ans: No, SHA-3 is not vulnerable to “length-extension attacks”

***If we use SHA-3 as a hash function, is H(K || message) a secure message authentication code?**

Explain.

Ans. SHA-3 is secure message authentication code.

1. SHA-3 takes an input of arbitrary length to produce output of desired length.

2. So, Receiver will be able to identify the modification to the message.

3. It would be impossible for attacker to generate a hash same as the original message after modification because the whole message is given at a time to generate the hash. So, block-wise hashing won’t work here.

Q4. Signing and Public-Key decryption 30%

The Decrypted file contained: Hasabe Swapnil today your lucky number is 501

Q5. **One-Time Pad 20%**

Q.5.

if $Pr[M=m] = \frac{1}{2^l}$ then $Pr[C=c \mid M=m] = \frac{1}{2^l}$

We have uniformly random key

$k \leftarrow \{0,1\}^l$ with same size of message $|M| = l$.

$C = M \oplus k$ and $M = C \oplus k$

By Definition of security: for all distribution over the message space, all m & all c:

$$Pr[M=m \mid C=c] = Pr[M=m]$$

Also, $Pr[C=c \mid M=m] = Pr[k = c \oplus m] = \frac{1}{2^l}$ — ①

$$Pr[C=c \mid M=m] = \frac{Pr[C=c, M=m]}{Pr[M=m]} \quad \text{(Conditional Probability)}$$

$$= \frac{Pr[M=m \mid C=c]\, Pr[C=c]}{Pr[M=m]}$$

$$= \frac{Pr[M=m \mid C=c]\, Pr[C=c]}{\sum_i (Pr[M=m \mid C=i]\, Pr[C=i])}$$

$$= \frac{Pr[M=m \mid C=c]\, Pr[C=c]}{Pr[M=m \mid C=c] \sum_i Pr[C=i]} \quad \text{But } \sum_i Pr[C=i] = 1$$

$$= Pr[C=c] \quad \text{— ②}$$

$$Pr[C=c] = \sum_{k,m} Pr(C=c \mid M=m, K=k) \cdot Pr(M=m, k=k)$$

$$= \sum_{k,m} Pr[M=m, k=k]$$

$$= \sum_{m} Pr[M=m] \cdot Pr[K = c \oplus m] \quad \text{(k is independent of m)}$$

$$= \frac{1}{2^l} \sum_m Pr[M=m] \quad \text{by ①} \quad \text{k is uniform}$$

$$\boxed{Pr[C=c] = \frac{1}{2^l}} \quad \text{— ②}$$

By ② + ③

If $Pr[M=m] = \frac{1}{2^\ell}$ then.

$$Pr[C=c \mid M=m] = \frac{1}{2^\ell}$$

Q6. **ElGamal Encryption 10%**

Q.6

Given, $C_1 = g^r$ is the first part of the ciphertext

$C_2 = h^r \cdot m$ is the 2nd part of the ciphertext.

Key Generation: Choose large prime p & $g \in Z_p^*$

Choose $x \in \{0, \ldots p-2\}$, set $h = g^x$ ——— eq^n (1)

Public key = (p, g, h) ; private key = x.

Decryption of received ciphertext is given by.

$$m \equiv C_2 (C_1^x)^{-1} \bmod p$$

$$\Rightarrow \frac{C_2}{C_1^x} = \frac{m \cdot h^r}{(g^r)^x}$$

$$= \frac{m \cdot (g^x)^r}{g^{rx}} = \frac{m \cdot g^{rx}}{g^{rx}} \qquad \text{put } h = g^x$$

$$\Rightarrow \frac{C_2}{C_1^x} = m \qquad \ldots\ldots \text{ hence the proof}$$

Q7. “Vanilla” RSA Encryption 10%

Q.7. "Vanilla" RSA Encryption 10%

Given Primes are $p=47$, $q=71$

Publickey $(N,e) = (3337, 79)$

$\phi(N) = (p-1)(q-1) = 3220$

We know, $ed = 1 \bmod \phi(N)$, we will check it with every option

(a) $e \cdot d \equiv 1 \bmod \phi(N)$

$79 \cdot 128 \not\equiv 1 \bmod \phi(N)$

(b) $e \cdot d \equiv 1 \bmod \phi(N)$

$\Rightarrow 79 \cdot 1019 \equiv 1 \bmod 3220$

$\Rightarrow 80501 \equiv 1 \bmod 3220$

(c) $e \cdot d \equiv 1 \bmod \phi(N)$

$79 \cdot 79 \not\equiv 1 \bmod 3220$

(d) $e \cdot d \equiv 1 \bmod \phi(N)$

$79 \cdot 2059 \not\equiv 1 \bmod 3220$

So, private key $\boxed{d = 1019}$ — Answer

or we can calculate d by using Extended Euclidean Algo. also.

Part I

$d \equiv e^{-1} \bmod 3220$

$\equiv 79^{-1} \bmod 3220$

Applying Euclidean Algo.

$\gcd(79, 3220) = 1$

$3220 = 79 \times 40 + 60$

$79 = 60 \times 1 + 19$

$60 = 19 \times 3 + 3$

$19 = 3 \times 6 + 1$

$\Rightarrow 1 = 19 + [-6] \cdot 3$

$\Rightarrow 3 = 60 + [-3] \cdot 19$

Put this value in above equation,

We will get;

$1 = 1019(79) + 25(3220)$

$79 \cdot 1019 \equiv 1 \bmod 3220$

$\Rightarrow \boxed{d = 1019}$ Answer

Part II, Given encrypted msg $= 1570 = c$

$m \equiv c^d \bmod N$ where $d = 1019$

$m \equiv (1570)^{1019} \bmod 3337$

Applying Fast Exponention,

$1570^2 \bmod 3337 \equiv 2194 \bmod 3337$

$1570^2 \cdot 1570^2 \bmod 3337$

$\equiv 2194 \cdot 2194 \bmod 3337$

$\Rightarrow m \equiv (1570)^{1019} \bmod 3337$

$\Rightarrow m \equiv 688 \bmod 3337.$

$\Rightarrow$ Plaintext message

$\boxed{m = 688}$ Answer