CS161–Spring 2015 — Solutions to Homework 3

Quoc Thai Nguyen Truong, SID 24547327, `cs161-di`

April 22, 2015

Collaborators: God

Problem 1

(a) $\boxed{False}$
Not all, some hash functions can be inverted.

(b) $\boxed{True}$

(c) $\boxed{True}$

(d) $\boxed{False}$
one-time pad also to be random and secret.

(e) $\boxed{False}$
In CBC mode, each block depends on the proper encryption of the previous block.

(f) $\boxed{False}$
If the attacker knows the symmetric-key, he can tamper with the message.

Problem 2

(a)

$$S^e = M \ mod \ n$$

$$e = 3, \ n \ is \ public$$

(b) Knowing $S^e = Mmodn$, I can write: $S^eM = kn$.
Given e, choose a random k, and S, I can find $M = S^e - kn$.
Therefore, Mallory can able to send that (S,M) to Bob.

(c) Bid $= S^e = S^3 \ mod \ n$

$$b = (S')^e = (S')^3 = 64 \cdot S^3 \ mod \ n$$

$$(S')^3 = 64 \cdot S^3 = (4 \cdot S)^3$$

(d) $\boxed{NO}$
In fact, the message is not only decry-pt integer, the public key is much very big, and the primes p and q will take a lot of time to be factors.

Problem 3

(a) USERTrust RSA Certification Authority → InCommon RSA Server CA → auth.berkeley.edu

(b) AddTrust AB

(c) Begin: Sunday, March 29, 2015 at 5:00:00 PM Pacific Daylight Time
End: Thursday, March 29, 2018 at 4:59:59 PM Pacific Daylight Time

(d) 256 bytes : 13 E5 A5 AB BA BE 5D 65 AC 39 07 42 B5 A0 CF 1D 2C BA 2B FB C0 15 0C B5 0B 91 CA 6B A3 32 3D 77 4A 02 CB 9D 1F 85 34 FF AB 9F A4 2F F6 B7 BB DF 86 B7 98 A2 6F 8D ED 49 26 C1 42 E0 09 BF 11 F8 A9 0C 53 08 B2 96 5C D3 69 77 3A 9F D9 CD B4 9C DA F6 96 F0 07 14 86 0C 56 B4 84 31 E5 8B 59 99 D8 62 87 D7 38 E4 18 FD DD 14 FE 1C 5C 2A C8 7F 02 CD 31 05 BF F3 5B A8 0C 48 1F 8A 7E CA 1A CA E3 2E D4 35 B6 8E 65 59 64 ED A5 37 19 FE 7D 8F E2 D6 F6 A0 53 D1 FE 54 64 74 55 38 AA 5A 26 F1 5D 6C 2B 64 95 22 D5 6D AF AE 40 00 19 39 92 8D 71 7D 5B B2 B6 8A A8 BE 0C 16 CE C6 FE 62 FC BC 6B 97 65 D8 23 34 49 EC 3D 26 52 B7 58 02 A5 2C 71 FC 67 B6 DD 75 99 55 CC A1 F4 D1 A8 4D C4 6F E4 F3 9D F4 08 C6 7F A8 87 73 74 A5 45 E5 A0 56 CE 1B 38 49 C0 B0 EC B8 8A 3F 0A B3 04 30 90 B5

Problem 4

$$n = 5,352,499 = 1237 \times 4327$$

$$(p-1)(q-1) = (1237-1) \times (4327-1) = 5,346,936$$

$$5d = 1 \; mod \; 5,346,936 => d = 4,277,549$$

$$C_1 = 4,784,648 \rightarrow M_1 = 4,784,648^{4,277,549} mod \; 5,352,499 => \boxed{M_1 = 120}$$

$$C_2 = 1,933,497 \rightarrow M_2 = 1,933,497^{4,277,549} mod \; 5,352,499 => \boxed{M_2 = 1,415}$$

$$C_3 = 4,437,506 \rightarrow M_3 = 4,437,506^{4,277,549} mod \; 5,352,499 => \boxed{M_3 = 1,514}$$

Problem 5

(a) *NO Good*
Explain: Everyone can intercept because they can know KB and KA. Hence, breaking rule number 4. Therefore, in order to fix this, both A and B needs to sign T with their private key.

(b) *NO Good*
Explain: Because Bob knows K1.

(c) *Good*

(d) *Good*

(e) *Good*

Problem 6

$$(x_0, y_0) = (1, 3);\ (x_1, y_1) = (2, 3);\ (x_2, y_2) = (5, 4)$$

$$l_0 = \frac{x - x_1}{x_0 - x_1} \times \frac{x - x_2}{x_0 - x_2} = \frac{x-2}{1-2} \times \frac{x-5}{1-5} = \frac{1}{4}x^2 - \frac{3}{2}x + \frac{5}{4}\ mod\ 7$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} \times \frac{x - x_2}{x_1 - x_2} = \frac{x-1}{2-1} \times \frac{x-5}{2-5} = -\frac{1}{3}x^2 + 2x - \frac{5}{3}\ mod\ 7$$

$$l_2 = \frac{x - x_0}{x_2 - x_0} \times \frac{x - x_1}{x_2 - x_1} = \frac{x-1}{5-1} \times \frac{x-2}{5-2} = -\frac{1}{12}x^2 - \frac{x}{4} + \frac{1}{6}\ mod\ 7$$

$$\rightarrow (l_0) \times y_0 + (l_1) \times y_1 + (l_2) \times y_2$$

$$= (l_0) \times 3 + (l_1) \times 3 + (l_2) \times 4$$

$$= x^2 + x + \frac{19}{6}\ mod\ 7$$

$$\rightarrow \textit{the secret is } \frac{19}{6}\ mod\ 7 = \boxed{2}$$

Problem 7

(a)

Problem 8

(a) Name: sgb-sy.com

(b) 192.168.56.102

(c) Source IP: 192.168.56.102
Destination IP: 46.149.110.103
Source port: 1066
Destination port: 80

(d) Sequence number of packet #49: 11726

(e) Total HTTP POST requests: 5

(f) Domain: google.com
Resource: Cookie

Problem 9

(a) IP of DNS: 4.2.2.3

(b) Domain: zivvgmyrwy.3razbave.info

(c) 177

(d) It ends on packet #399.
The size of the PE file is = 129,024 bytes

Problem 10

Great!!!!!