01. AUG. 2011

Crypto 1 Review Exercise
(Former exam)

1.) a.)

1) $P(K_1 \oplus K_2 = 0)$
2) $P(K_1 \oplus K_2 = 1)$

K_2 \ K_1	0	1
0	$p/2$	$p/2$
1	$\frac{1-p}{2}$	$\frac{1-p}{2}$

1) $\Rightarrow P(K_1 \oplus K_2 = 0) = \frac{p}{2} + \frac{1-p}{2} = \frac{1}{2}$

2) $\Rightarrow P(K_1 \oplus K_2 = 1) = \dots = \frac{1}{2}$

$$\Rightarrow P(K_1 \oplus K_2) = \begin{cases} 0, & 1/2 \\ 1, & 1/2 \end{cases} \Rightarrow K_1 \oplus K_2 \sim U(0,1)$$

$K = K_1 \oplus K_2$
$C_1 = K \oplus M$ $\Rightarrow P(C_1) = \begin{cases} 0, & 1/2 \\ 1, & 1/2 \end{cases} \Rightarrow C_1 \sim U(0,1)$

b.) For all values of p, the system has perfect secrecy as $K = \frac{1}{|K|}$ (uniformly distr.) and $e(M,K)$ holds s.t. $\exists$ such a $k \in K$ so that the system has perfect secrecy

c.) $H(M \mid C_1) \overset{!}{\geq} H(K_2 \mid C_1)$

$$\begin{aligned} H(M \mid C_1) &= H(M, C_1) - H(C_1) \\ &= H(C_1 \mid M) + H(M) - H(C_1) \\ &= H(K_1 \oplus K_2) + H(M) - H(C_1) \\ &= 1 + 1 - 1 \\ &= 1 \end{aligned}$$

$$\begin{aligned} H(K_2 \mid C_1) &= H(K_2, C_1) - H(C_1) \\ &= H(C_1 \mid K_2) + H(K_2) - H(C_1) \end{aligned}$$

$= H(K_1 \oplus M) + H(K_2) - H(C)$

$= H(K_2) + 1 - 1$

$= H(K_2) < 1$ since $0 < p < \frac{1}{2}$

$\Rightarrow H(M|C) > H(K_2|C)$

$H(M) = 1$, $H(M|C) = 1$ $\Rightarrow H(M|C) = H(M)$

$\Rightarrow$ perfect secrecy

b.)

d.) $e: (K \oplus M_1, K \oplus M_2) = (C_1, C_2)$

$d: (K \oplus C_1, K \oplus C_2) = (M_1, M_2)$

$d(e(M, K), K) = d((K \oplus M_1, K \oplus M_2), K)$

$= (K \oplus K \oplus M_1, K \oplus K \oplus M_2) = (M_1, M_2)$

$\Rightarrow$ the system satisfies the former conditions for each message $m_i \in M$ and $K \in K$

e.) $H(M_1|C_1) = H(M_1) + H(K) - H(C_1)$

$H(M_1) = -\frac{1}{2}\log_2(\frac{1}{2}) - \frac{1}{2}\log_2(\frac{1}{2}) = 1$

$H(K) = \ldots = 1$

$H(C_1) = \ldots = 1$

$H(M_1|C_1) = 1$ $H(M_2|C_2) = 1$ //same arguments

f.) ~~$H(M, C) = H(M_1) + H(M_2) + H(K) + H(K) - H(C_1) - H(C_2)$~~

$= 2$

wrong - fix at end of these papers

Crypto 1 Review Exercise

$H(M|C) = H(M,C) - H(C) = 2 - 1 = 1$

$H(M) = H(M_1) + H(M_2) = 2$

$\Rightarrow$ The system has <u>no</u> perfect secrecy since $H(M|C) \neq H(M)$

$(1 \neq 2)$

2.)

a.) Generate subkey K_1 for $K = 0x\,B4\,7F$

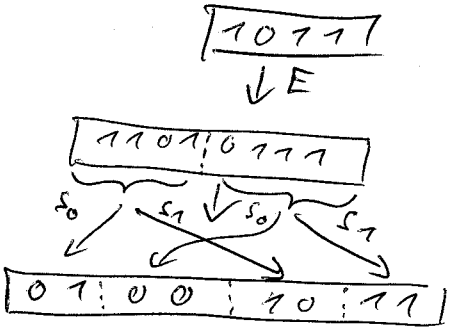
use $(K_1, K_2, K_3, K_4) = 0x\,B = 1011_2$

$E(K_1, K_2, K_3, K_4) = E(1011) = 11010111$

$S_0(1101) = 01$ $\quad S_1(1101) = 10$

$S_0(0111) = 00$ $\quad S_1(0111) = 11$

$K_1 = \underline{01001011} = 0x\,4B$



c.) Decryption procedure

1.) K_1, K_2, K_3, K_4 are generated

2.) IP on $C = (C_1, \dots, C_n) \Rightarrow \hat{C} = (\hat{C}_1, \dots, \hat{C}_n)$

3.) $\hat{M}_i = E_{K_i}(Z_i) \oplus \hat{C}_i = ROTL(Z_i \oplus K_i) \oplus \hat{C}_i$

4.) IP^{-1} on $\hat{M} = (\hat{M}_1, \dots, \hat{M}_4) \Rightarrow M = (M_1, \dots, M_n)$

Alternative solution: Analogous to encryption with M and C exchanged

b.) Compute IP^{-1}

5	6	7	8	4	3	2	1
13	14	15	16	9	10	11	12
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

} id. perm.

d.) Ciphertext $\hat{c}_1$ 10001100

$\hat{c}_2$ 11011001

$\hat{c}_3$ 11110101

$\hat{c}_4$ 01011011

$\hat{c}_1$ 10001100 = 0x38

IP 10011101 = 0x9D

11110101 = 0xF5

$\Rightarrow \hat{c}_4$ 01011011 = 0x5B

$\hat{m}_1 = ROTL(z_1 \oplus k_1, 4, 8) \oplus \hat{c}_1$

$z_2 \oplus k_2$

$z_3 \oplus k_3$

$\hat{m}_4 = z_4 \oplus k_4 \oplus \hat{c}_4$

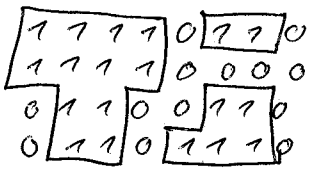
$z_1 = 4C$ $k_1 = 39$ $= 57 \oplus 38 = 6F$

$z_2 = 4D$ $k_2 = 64$ $= 92 \oplus 9D = 0F$

$z_3 = 4E$ $k_3 = 77$ $= 93 \oplus 5F = 66$

$z_4 = 4F$ $k_4 = 1C$ $= 35 \oplus 5B = 6E$

$\Rightarrow \hat{m} =$ 01101111 / 00001111 / 01100110 / 01101110

$IP^{-1} \Rightarrow$ 

e.) ECB, OFB, CBC, CFB, (CTR)

3.) $p = 11$, $q = 349$, $n = p \cdot q = 3839$

a.) mRPT on q:

$349 = 1 + q \cdot 2^k \Rightarrow 349 = 1 + 87 \cdot 2^k$

$\Rightarrow$ check if $3^{87} \not\equiv 1 \pmod{349}$

$3^{87} = (3^{10})^8 \cdot 3^7 \pmod{349}$

$\equiv 68^8 \cdot 93$

$= (68^2)^4 \cdot 93$

$= 87^4 \cdot 93$

$= 87^3 \cdot 87 \cdot 93$

Crypto 1 Review Exercise

$= 289 \cdot 64$

$= 348 = -1 \pmod{349} \neq 1$

$\Rightarrow$ 3 is not a strong witness

$\Rightarrow$ no, q is <u>not proven</u> to be prime

b.) $d = 37$

$e = d^{-1} \pmod{\varphi(n)} \rightarrow e = 37^{-1} \pmod{3480}$ ($\varphi(n) = 10 \cdot 348$)

<u>EEA:</u>

$3480 = 37 \cdot 94 + \underline{2}$

$37 = 2 \cdot 18 + \underline{1} \Rightarrow 1 = 37 - 2 \cdot 18$

$= 37 - (3480 - 37 \cdot 94) \cdot 18$

$= 37 \cdot \underbrace{1693}_{e} - 3480 \cdot 18$

$\Rightarrow e = 1693$

c.) $c = m^e \pmod{n} \equiv 44^{1693} \pmod{3839}$

Sq&M: $1693 \hat{=} 11010011101$

	44	(mod 3839)
1	S	1936
1	ms	1133
0	s	1463
1	ms	3047
0	s	1507
0	s	2200
1	ms	1122
1	ms	2596
1	ms	426
0	s	3608
1	m	1353

d.) You have $(d_1, e_1), \dots, (d_k, e_k)$

with $d_i \cdot e_i \equiv 1 \pmod{\varphi(n)} \quad \forall i = 1, \dots, k$

$\Rightarrow \varphi(n) \mid (d_i e_i - 1)$

If there is a unique common factor $\Rightarrow \varphi(n)$

i.e., calculate $\gcd(d_i e_i - 1, d_j e_j - 1) \quad i \neq j$

$\Rightarrow$ knowing n and $\varphi(n)$

solve $\left\{ \begin{array}{l} p \cdot q = n \\ (p-1)(q-1) = \varphi(n) \end{array} \right\}$ get p and q

e.) $(d_1 = 5, \; e_1 = 77)$ and $(d_2 = 13, \; e_2 = 37)$

$\Rightarrow d_1 \cdot e_1 - 1 = 5 \cdot 77 - 1 = 384$

$\Rightarrow d_2 \cdot e_2 - 1 = 13 \cdot 37 - 1 = 480$

$\left. \begin{array}{l} \gcd(384, 480) \\ = \gcd(384, 96) \\ = 96 \end{array} \right\} \; // \; 384 = 96 \cdot 4$

$\Rightarrow \varphi(n) = 96$

$p \cdot q = n = 119$

$\Rightarrow \varphi(n) = p \cdot q - p - q + 1 = 96$

$\Rightarrow 0 = n - p - \frac{n}{p} + 1 - \varphi(n)$

$\Rightarrow 0 = np - \varphi(n) p - p^2 - n + p$

$0 = p^2 - \underbrace{(n - \varphi(n) + 1)}_{:= a} p \underbrace{+ n}_{:= b}$

$(p, q) = \frac{-a}{2} \pm \sqrt{\left(\frac{a}{2}\right)^2 - b}$ $\qquad a = -24, \; b = 119$

$= 12 \pm \sqrt{144 - 119}$

$= 12 \pm 5 \Rightarrow p = 17, \; q = 7$

check $p \cdot q = n$ ...

$\varphi(n) = \dots$

1.f.1 fix

$$\begin{aligned} H(M,C) &= H(M,C,K) \\ &= H(M,K) \\ &= H(M_1,M_2,K) \\ &= H(M_1)+H(M_2)+H(K) \\ &= \underline{3} \end{aligned}$$

$$\begin{aligned} H(M|C) &= H(M,C)-H(C) \\ &= H(M,C)-H(C_1,C_2) \\ &= H(M,C)-H(C_1)-H(C_2) \\ &= 3-1-1 \quad \underline{\underline{=1}} \end{aligned}$$

According to e-mail.