CS427.

HW 1

Zongyan Lu.

1.

1.4 No. Bitwise-AND does not a good encryption method.

Compare with Bitwise-XOR.

The AND operator has 25% create 0
75% create 1.

Bitwise-AND

0 & 0 = 0
0 & 1 = 0
1 & 0 = 0
1 & 1 = 1

But Bitwise-XOR has equal possibility to generate either 0 or 1 uniformly.

Bitwise-XOR.

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$.

So, we say otp using XOR operation is special.
And AND-operation does not a good choice for encryption.

1.7. Based on equation. $\begin{cases} m_1 \oplus k = c_1 \\ m_2 \oplus k = c_2 \end{cases}$ So. $m_1 \oplus k \oplus m_2 \oplus k = c_1 \oplus c_2$
$\Rightarrow m_1 \oplus m_2 = c_1 \oplus c_2$.

c_1 = 1111 1001 0111 1001 1100 1100 0001 0111 1000 0110

$\oplus$ c_2 = 1111 1010 0110 0111 1101 1101 0000 1001 1000 1000

$c_1 \oplus c_2$ 0000 0011 0001 1110 0001 0001 0001 1110 0000 1110

Case I.

m_1 = alpha.

0000
8421

a: 6 1 → 0110 0001
l: 6 c → 0110 1100
p: 7 0 → 0111 0000
h: 6 8 → 0110 1000
a: 6 1 → 0110 0001

m_2 = bravo.

b: 6 2 → 0110 0010
r: 7 2 → 0111 0010
a: 6 1 → 0110 0001
v: 7 6 → 0111 0110.
o: 6 F → 0110 1111

So. $m_1 \oplus m_2 =$ 0110 0001 0110 1100 0111 0000 0110 1000 0110 0001

$\oplus$ 0110 0010 0111 0010 0110 0001 0111 0110 0110 1111

0000 0011 0001 1110 0001 0001 0001 1110 0000 1110

$\therefore m_1 \oplus m_2 = c_1 \oplus c_2$ when $\begin{cases} m_1 = \text{alpha} \\ m_2 = \text{bravo} \end{cases}$

Case 2.

m_1 = delta

d		e		l		t		a	
6	4	6	5	6	c	7	4	6	1
0110	0100	0110	0101	0110	1100	0111	0100	0110	0001

m_2 = gamma.

g		a		m		m		a	
6	7	6	1	6	d	6	d	6	1
0110	0111	0110	0001	0110	1101	0110	1101	0110	0001

So. $m_1 \oplus m_2 =$ 0110 0100 0110 0101 0110 1100 0111 0100 0110 0001

$\oplus$ 0110 0111 0110 0001 0110 1101 0110 1101 0110 0001

0000 0011 0000 0100 0000 0001 0001 1001 0000 0000

$c_1 \oplus c_2$ 0000 0011 0001 1110 0001 0001 0001 1110 0000 1110

$\therefore$ $m_1 \oplus m_2 \neq c_1 \oplus c_2$ when $\begin{cases} m_1 = \text{delta} \\ m_2 = \text{gamma} \end{cases}$

Hence. The plaintext alpha and braro. take the Same value by. xor gate calculation.

And plaintext delta and gamma doesn't.

So The correct encryption messages are.

$m_1 = \text{alpha}$. $m_2 = \text{bravo}$.

Based on this, the encryption key.

$k = m_1 \oplus c_1$: 0110 0001 0110 1100 0111 0000 0110 1000 0110 0001

$\oplus$ 1111 1001 0111 1001 1100 1100 0001 0111 1000 0110

key $\longrightarrow$ 1001 1000 0001 0101 1011 1100 0111 1111 1110 0111

2.8. $\mathcal{K} = \{1, \ldots, 9\}$.
$\mathcal{M} = \{1, \ldots, 9\}$.
$\mathcal{C} = \mathbb{Z}_{10}$

KeyGen:
$k \leftarrow \{1, \ldots, 9\}$.
return k

Enc(k, m):
return $(k \times m) \% 10$.

Based on two One-time Secrecy libraries:

we say.

$\mathcal{L}^{\Sigma}_{\text{ots-L}}$

EAVESDROP$(m_L, m_R \in \Sigma.\mathcal{M})$.
$k \leftarrow \{1, \ldots, 9\}$.
$c \leftarrow (k \times m_L) \% 10$
return c.

$\mathcal{L}^{\Sigma}_{\text{ots-R}}$

EAVESDROP$(m_L, m_R \in \Sigma.\mathcal{M})$
$k \leftarrow \{1, \ldots, 9\}$
$c \leftarrow (k \times m_R) \% 10$
return c.

And we construct a program $\mathcal{A}$.

$\mathcal{A}$.

$c \leftarrow$ EAVESDROP$(1, 2 \in \Sigma.\mathcal{M})$.
return $c \stackrel{?}{=} 1$

Based on the key and message. we get possibility table:

m \ k	1	2	3	4	5	6	7	8	9
1	1_1	2_2	3_3	4_4	5_5	6_6	7_7	8_8	9_9
2	2_2	4_4	6_6	8_8	10_0	12_2	14_4	16_6	18_8
3	3_3	6_6	9_9	12_2	15_5	18_8	21_1	24_4	27_7
4	4_4	8_8	12_2	16_6	20_0	24_4	28_8	32_2	36_6
5	5_5	10_0	15_5	20_0	25_5	30_0	35_5	40_0	45_5
6	6_6	12_2	18_8	24_4	30_0	36_6	42_2	48_8	54_4
7	7_7	14_4	21_1	28_8	35_5	42_2	49_9	56_6	63_3
8	8_8	16_6	24_4	32_2	40_0	48_8	56_6	64_4	72_2
9	9_9	18_8	27_7	36_6	45_5	54_4	63_3	72_2	81_1

So. $\Pr[A \diamond \mathcal{L}^{\Sigma}_{ots\text{-}L} \Rightarrow 1] = 1/9$.

$\Pr[A \diamond \mathcal{L}^{\Sigma}_{ots\text{-}R} \Rightarrow 1] = 0/9$.

Which $\Pr[A \diamond \mathcal{L}^{\Sigma}_{ots\text{-}L} \Rightarrow 1] \neq \Pr[A \diamond \mathcal{L}^{\Sigma}_{ots\text{-}R} \Rightarrow 1]$.

So, for pick message $m_L = 1, m_R = 2$
Which comes from secure scheme.
They demonstrate different possibilities
by constructing program A. When
linked to the two libraries from
ots.
This is contradicted with the definition of
ots. which the cipertext has same distribution
possibilites for any input from secure scheme.
So. we conclude this encryption algorithm does
not satisfy the definition of one-time secrecy.