CS2107 AY20/21 Sem 1 Mid-Term

A1. c

A2. a

A3. d

A4. c

A5. e

B1. Kerckhoffs' principle

B2. Mode-of-operation

B3. Initial Value (IV)

B4. MAC

B5. stream cipher

B6. Denial of service

B7. skimming

B8. Certification Authority

B9. Man-in-the-middle

B10. signature

C1. a) key space size = $\underline{2^{88}}$

b) testing 1 key takes 1024 = 2^{10} clock cycles

To check all 2^{88} keys, operation takes $2^{10} \cdot 2^{88} = 2^{98}$ clock cycles

4GHz dual-core processor has $2 \cdot 2^{2} \cdot 2^{30} = 2^{33}$ clock cycles per second

processor needs $\frac{2^{98}}{2^{33}} = 2^{65}$ seconds

$\approx 2^{40}$ years

$\approx$ **1T years**

C2. a)

$T = 2^{88}$

To have a probability more than 0.5 that a collision occurs,

find $M > 1.17\sqrt{T}$ $\Rightarrow$ $M = 2 \cdot \sqrt{2^{88}}$

$= \underline{2^{45}}$

b)

hash function takes $512 = 2^{9}$ clock cycles to generate digest

To generate 2^{45} digests, operation takes $2^{9} \cdot 2^{45} = 2^{54}$ clock cycles

1024 servers, each with quad core 4GHz processor has $2^{10} \cdot 2^{2} \cdot 2^{2} \cdot 2^{30}$

$= 2^{44}$ clock cycles per second

time needed $= \frac{2^{54}}{2^{44}} = 2^{10}$ seconds

$\approx \frac{1}{4}$ hour

$\approx$ $\underline{15 \text{ minutes}}$

C3. a) i) $n = pq$

$= \underline{187}$

ii) $\phi(n) = (p-1)(q-1)$

$= \underline{160}$

iii) $e \cdot d = 1 \pmod{\phi(n)}$

only $d = 107$ $\Rightarrow$ $3 \cdot 107 = 321 = 1 \pmod{160}$

b)

$$((3m)^e)^d = 3m \pmod n$$

$$(3^e \cdot m^e)^d = 3m \pmod n$$

$$(3^e \cdot c)^d = 3m \pmod n$$

multiply c by 3^e (e is from public key)

need prove?

$$3^{ed} = 3^{k\phi(n)} \cdot 3$$
$$= 3 \pmod n$$

C4.

$$c \oplus k = \text{From: Bob}$$

$$c \oplus ? \oplus k = \text{From: Bot}$$

```
    F r o m :   B o b
xor 0 0 0 0 0 0 0 0 ?
---------------------
    F r o m :   B o t
```

$b \oplus t = ?$

```
    01100010
xor 01110100
------------
    00010110
```

Mallory can xor the 9th byte of ciphatext with <u>00010110</u>