1) $n = pq$ $\quad h(x) = x^2 \bmod n$ $\quad \phi_n = (p-1)(q-1)$

a) whis is h preimage resistant

to find x $\quad d \in \mathbb{Z}$ $\exists$ $(x^2)^d = x \bmod n$

$\Rightarrow x^{2d} = x \bmod n \quad \Rightarrow 2d = 1 \bmod \phi(n)$

because $\phi(n), 2 \neq 1$

$\Rightarrow$ it is preimage resistant because we have to first find the product of integers to find x

b) why is h not collission resistant?

suppose $x_n \to n \in \mathbb{Z}^* \Rightarrow (x+h)^2 = x^2 = 2nx + h^2 = x^2 \bmod n$

$\Rightarrow x + h \neq h$ but $h(x) = h(x+h)$

---

2) a) 256 bits long binary strig $\quad$ avg success probability of 0.75 $\quad M = 2^{256} \quad Q = ?$

$(\varepsilon) = 0.75$

(ε) prob of hash $= 1 - e^{\frac{-Q(Q-1)}{2M}}$

$\Rightarrow$ assuming $(Q^2 - Q) = Q^2 \Rightarrow Q \approx \sqrt{2M \ln\left(\frac{1}{1-\varepsilon}\right)}$

$Q \approx 4.0065\, \varepsilon^{38}$

2b) $h(m) = m_1^a m_2^b \bmod n$ a int rel. prime to ϕ_n and b chosen $\Rightarrow$ $ab = 1 \bmod \phi_n$

$m_1, m_2 \in Z_n$ m as an input

$m = m_1 \| m_2$ $h(m) = m_1^a m_2^b \bmod n$

Find 2nd preimage

1) $y \leftarrow h(x)$
2) choose $X_0 \subseteq X - \{x\}$ with $|X_0| = e^{-1}$
3) for each $x_0 \in X_0$ do
4) if $h(x_0) = y$ return x_0
5) return fail

any success for 2nd preimage: $\varepsilon = 1 - (1 - \frac{1}{n})^{e-1}$

For 2b it IS preimage resistant because it is a one-way cryptographical equation. It is relatively "hard" to solve because the hacker has to solve for both a and b

2c) $h_1 = h_0^a \cdot m_1^b \bmod n$
$h_2 = h_1^a \cdot m_1^b \bmod n$

IS NOT preimage resistant because the two messages have both the same a, b values $\Rightarrow$ they can find a 2nd message that produces the same hash value as the 1st message making it susceptible to attacks

3) fam = 4 $\quad$ $n = 12$

Bday problem

prob 2nd person has diff bday month is $\frac{12-1}{12} = 1 - \frac{1}{12}$

3rd person has diff bday is $1 - \frac{2}{12}$

4th person is $1 - \frac{3}{12}$

$$Pr(\text{diff bday months}) = \prod_{i=1}^{Q-1} \left(1 - \frac{i}{12}\right) \leq e^{-\frac{Q(Q-1)}{2n}} \qquad n = 12,\ Q = 4$$

$$\left(1 - \frac{1}{12}\right)\left(1 - \frac{2}{12}\right)\left(1 - \frac{3}{12}\right) = 0.5729 \text{ (actual)}$$

$$e^{-\frac{4(4-1)}{2(12)}} = 0.6065 \text{ (approximation)}$$

---

4) 4 parties: A, B, C, D $\quad$ large prime p $\quad$ primitive root α

privately chosen a, b, c, d

ignore the next in the middle

A = Alice
B = Bob
C = Charles
D = Doug

$$K = \alpha^{abcd} \bmod p$$

protocol to securely compute (K ignore next in the middle)

use Diffie-Hellman

i) p & α public values

a^{-1} is mult inverse of $a \bmod p-1$
b^{-1} is mult inverse of $b \bmod p-1$
& so on

- Alice computes $A = \alpha^a \bmod p$ and sends to Bob.
- Bob computes $B = A^b = \alpha^{ab} \bmod p$ and sends to Charles
- Charles computes $C = B^c = \alpha^{abc} \bmod p$ and sends to Doug
- Doug computes $D = C^d = \alpha^{abcd} \bmod p$ and sends to Alice
- Alice computes $K_A = D^{a^{-1}} \bmod p$ where a^{-1} is inverse of $a \bmod p-1$ ($K_A = \alpha^{bcd} \bmod p$) and sends to Bob
- Bob computes $K_B = K_A^{b^{-1}} \bmod p = \alpha^{cd \pmod{p-1}}$ and sends to Charles
- Charles computes $K_C = K_B^{c^{-1}} \bmod p = \alpha^d \bmod p$ and sends to Doug
- Doug computes $K_D = K_C^{d^{-1}} \bmod p = \alpha \bmod p$

Alice has $A = \alpha^a \bmod p$ & $K_A = \alpha^{bcd} \Rightarrow K_A \cdot A = \alpha^{abcd} \bmod p = K$

Bob has $B = \alpha^{ab} \bmod p$ and $K_B = \alpha^{cd} \bmod p \Rightarrow B \cdot K_B = \alpha^{abcd} \bmod p = K$

Charles has $C = \alpha^{abc} \bmod p$ & $K_C = \alpha^d \bmod p \Rightarrow C \cdot K_C = \alpha^{abcd} \bmod p = K$

Doug has $D = \alpha^{abcd} \bmod p = K$ $\Rightarrow$ all members have the same K

5) $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ $\quad h_2 : \{0,1\}^{4m} \to \{0,1\}^m$

a) $x \in \{0,1\}^{4m}$ as $x_1 || x_2$ where $x_1, x_2 \in (0,1)^{2m}$

b) define $h_{(2)}(x) = h_1(h_1(x_1) || h_1(x_2))$

h_1 assumed collision resistant

Assume ~~[illegible]~~ h_2 is NOT collision resistant

$\Rightarrow$ that exists $x_1, x_2 \in \{0,1\}^{4m}$ such that $x_1 \neq x_2$ but $h_2(x_1) = h_2(x_2)$

$\Rightarrow$ there exists $x = x_1 || x_2$ & $y = y_1 || y_2$ in $(0,1)^{4m}$

$*$ such that $x \neq y$ but $h_2(x) = h_2(y)$

$\Rightarrow h_2(x) = h_1(h_1(x_1) || h_1(x_2))$ $\quad h_2(y) = h_1(h_1(y_1) || h_1(y_2))$

$\Rightarrow h_2(x) = h_2(y) \Rightarrow h_1(h_1(x_1) || h_1(x_2)) = h_1(h_1(y_1) || h_1(y_2))$

$\Rightarrow$ because h_1 collision resistant $h_1(a) = h_1(b) \Rightarrow a = b$

$\Rightarrow$ (a) $h_1(x_1) || h_1(x_2) = h_1(y_1) || h_1(y_2) \Rightarrow h_1(x_1) = h_1(y_1)$ & $h_1(x_2) = h_1(y_2)$

$\Rightarrow$ because h_1 is collision resistant and $h_1(x_1) = h_1(y_1) \Rightarrow x_1 = y_1$ & $x_2 = y_2$

$\Rightarrow$ because $x_1 = y_1$ & $x_2 = y_2 \Rightarrow x = y$ and $h_2(x) = h_2(y)$ $*$

which contradicts our previous statement $x \neq y$ but $h_2(x) = h_2(y)$

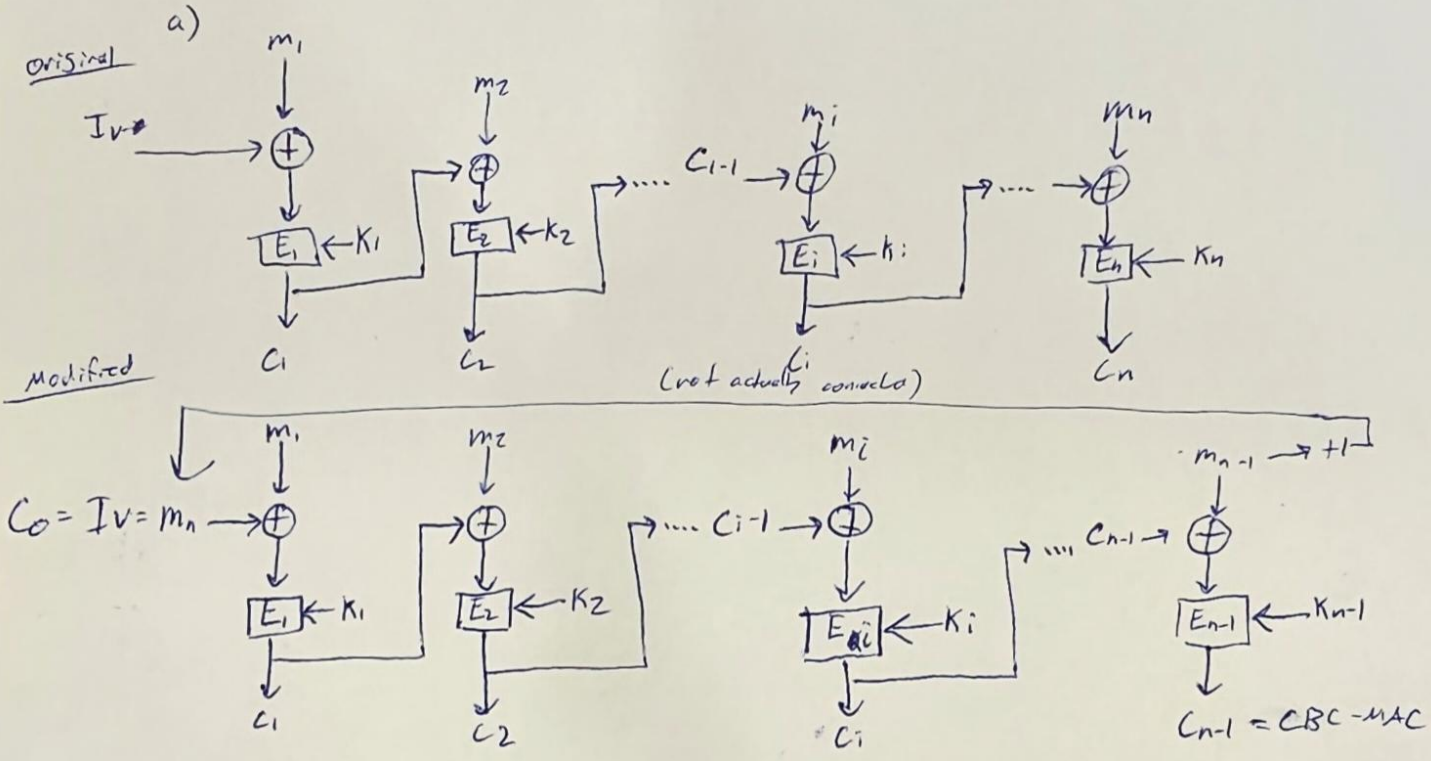
$\Rightarrow$ our assumption h_2 is Not collision resistant is false & is

Collision Resistant

6) CBC-MAC original: $C_i = E_K(C_{i-1} \oplus m_i)$ for $i = 1, 2, \ldots n$

modified: $C_i = E_K(C_{i-1} \oplus m_i)$ for $i = 1, 2, \ldots n-1$

a)



b) in the original CBC-MAC the IV is a block of zeroes and in the modified it is $m_{n-1} \Rightarrow C_{i(original)} \neq C_{i(new)}$

Inductively deduce

assume $n = K$

$\Rightarrow$ original CBC-Mac outputs C_n & modified outputs C_{n-1} *$(C_{K+1-1} = C_K)$

$\Rightarrow$ now assume $n = K+1$ $\Rightarrow$ original CBC MAC outputs $C_{K+1} = E_K(C_K \oplus m_{K+1})$

$\Rightarrow$ modified CBC MAC outputs $C_{K+1-1} = E_K(C_{K-1} \oplus m$

*(m_{K+1-1}) for modified

* no C_{K+1} for modified

~~$\Rightarrow$ even when adding~~

C_i

$\Rightarrow C_{K(original)} \neq C_{(modified)}$ & even when adding another block to make $n = K+1$ the method of adding is different

$\Rightarrow$ NOT THE SAME output