Assignment 4

Thursday, December 1, 2021 12:26 AM

1. n=pq $f(x) = x^2 \pmod n$

a. to solve for preimage x, need to find x that satisfies
$f(x) = x \pmod n$

$d \in \mathbb{Z}$ $(x^2)^d \equiv x \pmod n$

$2d \equiv 1 \pmod{\phi(n)}$

$\phi(n) = (p-1)(q-1)$ is two one numbers multiplied

and so $\gcd(\phi(n), 2) \neq 1$ and finding x is not easily computed

so it is preimage resistant

b. Given x_1, consider $x_2 = x_1 + 2 \in \mathbb{Z}^*$

$x^2 = (x+2)^2 \pmod n$

$(x+2)^2 = x^2 + 2x + 2^2 = x^2 \pmod n$

so $x + 2 \neq x$, but $f(x+2) = f(x)$

so f is not collision resistant

2a. $Q = \sqrt{2M\ln\left(\frac{1}{1-\alpha}\right)}$ for minimum

$Q = \sqrt{2(2^{128})\ln\left(\frac{1}{1-0.75}\right)} = 5.67 \cdot 10^{38}$

b. n=pq a random prime to $f(n)$ also ϕ mod ϕn

$m_1, m_2 \in \mathbb{Z}_n$ $m = m_1 \| m_2$ $f(m) = m_1^{2^k} m_2^{2^k} \bmod n$

To show 2^k preimage, need to find m' that isn't congruent to m but still gives $f(m') = f(m)$

$m' = m_2^{2^k} \| m_1^{2^k} \rightarrow$

since $x^{2^k} = x \bmod n$ for any x as $2^k \equiv 1 \bmod \phi(n)$

so $m \neq m'$
$m_1 \| m_2 \neq m_2^{2^k} \| m_1^{2^k}$

but $f(m') = f(m)$ as

$f(m') = m_2^{2^k} m_1^{2^k} \bmod n = m_1^{2^k} m_2^{2^k} \bmod n = f(m) = m_1^{2^k} m_2^{2^k} \bmod n$

so not 2^k preimage resistant

c. $m = m_1 \| m_2$

$h_1 = h_0^{m_1} \cdot m_1^2 \bmod n$ $h_2 = h_1^{m_2} \cdot m_2^2 \bmod n$

h_0 = fixed value (random prime)

$h(m) = h_2$

find $m' \neq m$ but $h(m') = h(m)$

$m' = m_2^2 \| m_1^2$ as $\phi(n) = 1 \bmod \phi(n)$
so $x^{\phi(n)} = x \bmod n$

$h(m') = (h_0^{m_2} \cdot m_2^2)^{m_1} \cdot m_1^2 \bmod n$

$= h_0^{m_2} m_1 m_2^2 \bmod n$

$h(m') = (h_0^{m_1} \cdot m_1^2)^{m_2} \cdot m_2^2 = h_0^{m_1} \cdot m_1 \cdot m_2^2 \bmod n$

so $h(m') = h(m')$

but $m = m_1 \| m_2 \neq m' = m_2^2 \| m_1^2$

3. family of four, prob no two people have birthdays in same month?

Prob(different birthday months) $= (1 - \frac{1}{12})(1 - \frac{2}{12})(1 - \frac{3}{12})$

$= 165/288 = 0.5729 \approx 0.573$

$= 57.3\%$

4. $h: X \rightarrow Y$ $(|X| = N, |Y| = M)$

$h^{-1}(y) = \{x : h(x) = y\}$ $s_y = |h^{-1}(y)|$ for $y \in Y$

$y = 1 - \frac{\binom{N-s_y}{q}}{\binom{N}{q}}$

$P_r(S) = 1 - P_r(F)$ $P_r(F) = \frac{|\text{number of fail}|}{|\text{number of try}|}$

try = choose q of N elements $= \binom{N}{q}$

fail = choose q of $(N - s_y)$ elements

$s_y = |h^{-1}(y)| \rightarrow |x : h(x) = y|$
$\rightarrow \{x : h(x) = y\}$

avoid all $x : h(x) = y$

$|\text{fail}| = \binom{N-s_y}{q} \rightarrow$ so $P_r(S) = 1 - \frac{\binom{N-s_y}{q}}{\binom{N}{q}}$

b. $\overline{P(S)} = 1 - \overline{P(F)}$

$\overline{P(F)} = \sum_{y \in Y} \frac{P_r(F)}{|y|}$

$\overline{P(S)} = 1 - \frac{\sum_{y \in Y} \frac{\binom{N-s_y}{q}}{\binom{N}{q}}}{M}$ $|y| = M$

$= 1 - \frac{1}{M} \sum_{y \in Y} \frac{\binom{N-s_y}{q}}{\binom{N}{q}}$

c. $q = 1$

$\overline{P(S)} = 1 - \frac{1}{M} \sum_{y \in Y} \frac{\binom{N-s_y}{1}}{\binom{N}{1}}$

$\binom{N}{1} = N$ for any N

$\overline{P(S)} = 1 - \frac{1}{M} \sum_{y \in Y} \frac{N - s_y}{N}$

$= 1 - \frac{\sum_{y \in Y} N - \sum_{y \in Y} s_y}{M \cdot N}$ $\rightarrow \sum s_y = N$

has M terms

$= 1 - \frac{MN - N}{MN}$

$= 1 - \frac{MN}{MN} + \frac{N}{MN} = 1 - 1 + \frac{1}{M}$

$\overline{P(S)}$ with $q = 1$ is $\frac{1}{M}$

5. $h_1 : \{0,1\}^{2m} \rightarrow \{0,1\}^m \rightarrow$ collision resistant

$h_2 : \{0,1\}^{4m} \rightarrow \{0,1\}^m$

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

$x_1 = x_1' \| x_1'' \rightarrow x_1', x_1'' \in \{0,1\}^{2m}$

$x_2 = x_2' \| x_2'' \rightarrow x_2', x_2'' \in \{0,1\}^{2m}$

since $h_2(x_1) = h_2(x_2)$

$h_1[h_1(x_1') \| h_1(x_1'')] = h_1[h_1(x_2') \| h_2(x_2'')]$

concatenation operation:

$h_1(x_1') = h_1(x_2')$

$h_1(x_1'') = h_1(x_2'')$

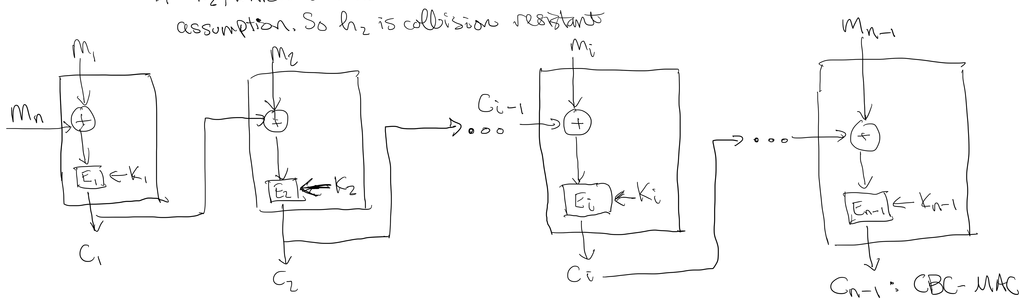
Since h_1 is collision resistant

$x_1' = x_2'$ and $x_1'' = x_2''$

meaning

$x_1 = x_2$, which contradicts initial assumption. So h_2 is collision resistant

6a.



b. for $n = 1$

with original CBC-MAC, the output is $C_1 = E_1(m_1, k_1)$

with new CBC-MAC, the output is $C_0 = m_1$ for base case

so output of modified and original are different

$C_n = E_n(C_{n-1} + m_n, k_n) \neq C'_{n-1} = E_{n-1}(C_{n-2} + m_{n-1}, k_{n-1})$

and C_1 for modified $= C_1 = E_1(m_1 + m_1, k_1)$
$n = 2$

7. Programming