10955003l 李昊融

HW #4

① $H(N_1 N_2) = Enc(IK, Enc(IK, N_1) \oplus N_2)$

$= Enc(IK, Enc(IK, N_1) \oplus Enc(IK, N_1) \oplus Enc(IK, M_1) \oplus M_2)$

$= Enc(IK, Enc(IK, M_1) \oplus M_2)$

$= H(M_1, M_2)$

$= h$

Thus, H doesn't satisfy the property of second image resistant #

② $f=0 \Rightarrow$ function: $\sin 0 = 0$

$0\times0 + 0\times1 + 0\times0 + 0\times3 + 0\times0 + 0\times1 + 0\times0 + 0\times3 = 0$ #

$f=1 \Rightarrow$ function: $\sin(\frac{\pi}{4}x)$

$\sin 0\cdot 0 + \sin(\frac{\pi}{4})\cdot 1 + 0 + \sin(\frac{3\pi}{4})\cdot 3 + 0 + \sin(\frac{5\pi}{4})\cdot 1 + 0 + \sin(\frac{7\pi}{4})\cdot 3 = 0$ #

$f=2 \Rightarrow$ function: $\sin(\frac{\pi}{2}x)$

$0 + \sin(\frac{\pi}{2})\cdot 1 + 0 + \sin(\frac{3\pi}{2})\cdot 3 + 0 + \sin(\frac{5\pi}{2})\cdot 1 + 0 + \sin(\frac{7}{2}\pi)\cdot 3 = -4$ #

$f=3 \Rightarrow$ function: $\sin(\frac{3}{4}\pi x)$

$0 + \sin(\frac{3}{4}\pi)\cdot 1 + 0 + \sin(\frac{9\pi}{4})\cdot 3 + 0 + \sin(\frac{15}{4}\pi)\cdot 1 + 0 + \sin(\frac{21}{4}\pi)\cdot 3 = 0$ #

③

$$e = 2{,}7182\cdots$$

$$= 2 + \cfrac{1}{\cfrac{1}{0{,}7182}} = 2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{0{,}3923}}} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{1}{0{,}549}}}}$$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{0{,}8214}}}}} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{0{,}2174}}}}}}$$

$$= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{0{,}599}}}}}} \approx 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}} = \frac{87}{32} = 2{,}71875\cdots$$

#

④

(a) $\left| \frac{d}{N} - \frac{k}{S} \right| < \frac{1}{2N} = \frac{1}{2048}$

$\Rightarrow d=85$, $\left| \frac{85}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{1}{12}$

$\Rightarrow d=171$, $\left| \frac{171}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{2}{12}$

$\Rightarrow d=341$, $\left| \frac{341}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{4}{12}$

$\Rightarrow d=427$, $\left| \frac{427}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{5}{12}$

$\Rightarrow d=512$, $\left| \frac{512}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{6}{12}$

$\Rightarrow d=597$, $\left| \frac{597}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{7}{12}$

$\Rightarrow d=683$, $\left| \frac{683}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{8}{12}$

$\Rightarrow d=853$, $\left| \frac{853}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{10}{12}$

$\Rightarrow d=939$, $\left| \frac{939}{1024} - \frac{k}{S} \right| < \frac{1}{2048} \Rightarrow \frac{k}{S} \approx \frac{11}{12}$

Thus, we can find S of $g(x)$ is 12

$7^{12} \bmod 39 = 1$, $7^{6} \bmod 39 = 25$

$25-1=24 \Rightarrow p = \gcd(39,24) = 3$
$25+1=26 \Rightarrow q = \gcd(39,26) = 13$ $\Rightarrow N = pq = 3 \times 13$ #

(b) probability:

$d=0 \Rightarrow p \approx 0.162$
$d=85 \Rightarrow p \approx 0.031$
$d=171 \Rightarrow p \approx 0.022$
$d=256 \Rightarrow p \approx 0.0002$
$d=341 \Rightarrow p \approx 0.022$
$d=427 \Rightarrow p \approx 0.013$
$d=512 \Rightarrow p \approx 0.054$
$d=597 \Rightarrow p \approx 0.013$
$d=683 \Rightarrow p \approx 0.022$
$d=768 \Rightarrow p \approx 0.0002$
$d=853 \Rightarrow p \approx 0.022$
$d=939 \Rightarrow p \approx 0.031$
$P_{total} \approx 0.3924$ #