			Date
	(5171	HW4	
011		V	for intinitaly man
(X1.1	suppose g(n) isn't negligible, i.e.	there exists some P(n) such that I	
	$\Omega$ , $g(n) = 2^{-f(n)} Z_{P(n)}$	120/0/11/11	
	laking log, both spoter; - the	22-1092 (P(n))	
	tostituting of (n)=Wlogn: VV logs	A TUSZ (TYAS)	<u> </u>
	f(n) = 101 (log n) means f(n)	> clogn for any c	
	$9(n) = 2 - f(n) = \frac{1}{2+m}$ where =	2+m < 2 (109n	
	* ~ 1 1 1 1 1		0/1/6/11/
	P(n) <n (for="" a<="" c="" td=""><td>my Polynomial p(n) there exits ( that</td><td>P(n) (n holds)</td></n>	my Polynomial p(n) there exits ( that	P(n) (n holds)
		的一个村村村一直上面相	
(31)	4(n) = 0 (1000) mass $4(n)$	) < c 60gm 1 3 4 1 5000 6 9	8 - 1 1-9
C(110	$g(n) = 2^{-f(n)} = \frac{1}{2^{+f(n)}}$ where	1 > 1 > 0	1=.2:
		2 to 2 Cog!	3 =
	9(n)>no	ppt in n, non-negligible.	
	$n^{5} > 9(n) (9(n) 1)$		9 ==
012	a) - 10/11-		A A
WI,5	[발생님 : [1] [1] [1] [1] [1] [1] [1] [1] [1] [1]	My Starte M. R. M. Whele M.	
b) negligible		Office O sings 3 30	
	() Non-negligible	Ligita I days	A 1T
		Mark to sently of F.	A YOU WILL
Q2. I-	F A Cannot break 0,1, it cannot	break 0,2 too.	
	· ' Given Pr [ (n)=1755	- + negl(n)	
	Since in 0,2, the adversary do	lein4 Know b: { Pr[HATT (n.0)=1] = Pr[ Pr[HATT (n.1)=1] = Pr[	GAM (n)=1] (=+ +neo
	50, Pr [HA,TI (17,0)=1]-Pr[HA	$\pi(n,1)=1]$ { $negl(n)$	
J	f A cannot bleak 012, It cannot	brak 0,1 too.	
	"Given IPr [HATT (n,0)=1]-Pr[+	1AT (n,1)=1]   Snegl(n)	
	Pr [GATI (n) = 1]= = EPr [HA,TI (1	n.0)=0]+==================================	
	ST (POTUL	(n,0)=0]+(Pr[HA,T(n,0)=1]+negl(n)))	
	( \f( 1 \tau neg		
	$\langle \frac{1}{2} \pm negl(n)$		
	( 2 1 1 6) 101	,	

23. XOR We know: Lo, $R_0 = L_1$ , $L_3$ , $R_3$ and $R_4$ where $R_1$ and $R_4$ with $R_4$ and	= (n) + (n) = (n) + (n) + (n) = (n) + (n) = (n
OOO O OII Wk, $\chi$ 1st bit of $f_k(\chi) = 1^{st}$ bit of $\chi$ abd and  Ne know:  After O): $L_1 = R_0$ ; $L_2^{st}$ bit of $R_1$ After C): 1st bit of $L_2^{st}$ ; $L_2^{st}$ bit of $R_2^{st}$ and $L_2^{st}$ bit of $R_2^{st}$ Let $L_{2,1}$ $L_{2,1}$ denote $L_2^{st}$ bit of $L_2^{st}$	= (n) + (n) = (n) + (n) = (n) + (n) = (n
OOO O OII Wk, $\chi$ 1st bit of $f_k(\chi) = 1^{st}$ bit of $\chi$ abd and  Ne know:  After O): $L_1 = R_0$ ; $L_2^{st}$ bit of $R_1$ After C): 1st bit of $L_2^{st}$ ; $L_2^{st}$ bit of $R_2^{st}$ and $L_2^{st}$ bit of $R_2^{st}$ Let $L_{2,1}$ $L_{2,1}$ denote $L_2^{st}$ bit of $L_2^{st}$	= (n) + (n) = (n) + (n) = (n) + (n) = (n
We know:  We know:  After a): $L_1=R_0$ ; $L_2$ bit of $R_1$ (a) After b): $L_3$ bit of $L_2$ ; $L_3$ bit of $L_3$ bit of $L_3$ bit of $L_3$ Let $L_{2,1}$ & $R_{2,1}$ denote $L_3$ bit of $L_3$ & $L_4$ & $L_5$ & $L$	= (n) + (n
We know:  We know:  After a): $L_1=R_0$ ; $L_2$ bit of $R_1$ (a) After b): $L_3$ bit of $L_2$ ; $L_3$ bit of $L_3$ bit of $L_3$ bit of $L_3$ Let $L_{2,1}$ & $R_{2,1}$ denote $L_3$ bit of $L_3$ & $L_4$ & $L_5$ & $L$	= (n) + (n) = (n) + (n) = (n) + (n) = (n
After 0): $L_1=R_0$ ; $L_2$ t bit of $R_1$ .  After b): It bit of $L_2$ ; $L_2$ t bit of $R_2$ .  After c): $L_1$ t bit of $L_2$ ; $L_2$ t bit of $L_3$ ; $L_2$ t bit of $L_3$ ; $L_3$ t bit of $L_4$ t $L_5$	
After 0): $L_1=R_0$ ; $L_2$ t bit of $R_1$ .  After b): It bit of $L_2$ ; $L_2$ t bit of $R_2$ .  After c): $L_1$ t bit of $L_2$ ; $L_2$ t bit of $L_3$ ; $L_2$ t bit of $L_3$ ; $L_3$ t bit of $L_4$ t $L_5$	
After a): $L_1=R_0$ ; $L_2=R_0$ ; $L_3=R_0$ ;	P
Let $L_{i,1}$ & $R_{i,1}$ denote $I^{ot}$ bit of $L_{i}$ & $R_{i}$ $I^{ot}$	P
Let $L_{i,1}$ & $R_{i,1}$ denote $I^{ot}$ bit of $L_{i}$ & $R_{i}$ $I^{ot}$	P
$= R_{1,1} \oplus (L_{1,1} \oplus R_{1,2})$ $= L_{1,1} \oplus (L_{1,1} \oplus R_{1,2})$ $= R_{0,1}$ $= R_{0,2}$ $\vdots A an query F with Mod M2 where Mo start with 0 l m2 start in If 1st bit of R3 (equals 0, output 0 (equals 1, output 2)$	P
$= R_{1,1} \oplus (L_{1,1} \oplus R_{1,2})$ $= L_{1,1} \oplus (L_{1,1} \oplus R_{1,2})$ $= R_{0,1}$ $= R_{0,2}$ $\vdots A an query F with Mod M2 where Mo start with 0 l m2 start in If 1st bit of R3 (equals 0, output 0 (equals 1, output 2)$	P
$= R_{1,1} \oplus (L_{1,1} \oplus R_{1,2})$ $= L_{1,1}$ $= R_{0,1}$ $= R_{0,2}$ $\therefore A \text{ an query } F \text{ with } M_0 \& M_2 \text{ where } M_0 \text{ starts with } 0 \& M_2 \text{ starts } V$ $If 1^{st} \text{ bit of } R_3 \text{ (equals } 0, \text{ output } 0$ $\text{ (equals } 1, \text{ output } 1$	
= L <sub>2,2</sub> = R <sub>0,2</sub> : A an query F with M. & M. where M. Starts with 0 & M. Starts with 0	
= Ro,2  A can query F with M. & M.z where M. Starts with 0 & M.z. Starts in If 1st bit of R.s. lequals 0, output 0  [equals 1, output 2]	
i. A an query F with M. & M. where M. Starts with 0 & M. Starts with 0	
This way, A break & security of F.	1990 (d
not broak 0,2, it count broak 0,2 too,  of PTG+ (6)=235++ real(6)	SVIN
10 0,2, the industry when there is 19 [12 (0,0) = 2] = [[[(0,0) + 2] (12 + 10 + 1)] = [[(0,0) + 1] = [(0,0) + 1)] = [(0,0) + 1)	
(a) Leaft. 10 12 - F. C. 12 - F. C. 12 - C. 12	No.
not plant of word of the state of	5 A RI
(A) INSUR [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [	
TE = (BA) = AH NET C= (BA) BAH NET = (BA)	
((n) psn = [t=10,0)maH3-1) + [b=(0-0)maH3-1) ==	
(m) (gn ±1)+>	
の別なります。	

No.

The second secon