11005480 易頡

15. $i=0$ $a_0=1$ $X=1900\cdot 1 \bmod 2537=1900$ $power=1900^2 \bmod 2537=2386$

$i=1$ $a_1=0$ $X=1900$ $power=2386^2 \bmod 2537=2505$

$i=2$ $a_2=1$ $X=1900\cdot 2505 \bmod 2537=88$ $power=2505^2 \bmod 2537=1024$

$i=3$ $a_3=1$ $X=88\cdot 1024 \bmod 2537=1317$

return $X=1317=1900^{13} \bmod 2537$

16 $i=0$ $a_0=1$ $X=210\cdot 1 \bmod 2537=210$ $power=210^2 \bmod 2537=971$

$i=1$ $a_1=0$ $X=210$ $power=971^2 \bmod 2537=1614$

$i=2$ $a_2=1$ $X=210\cdot 1614 \bmod 2537=1519$ $power=1614^2 \bmod 2537=2034$

$i=3$ $a_3=1$ $X=1519\cdot 2034 \bmod 2537=2117$

17. 將ATTACK轉為數字表示 00 19 19 00 02 10

$n=43\cdot 59=2537$，將轉換換後的數字4位為一組

因為 $2525<2537<252525$

第一組 0019 密文 $C=(0019)^{13} \bmod 2537=2299$ (根據第14題)

第二組 1900 密文 $C=(1900)^{13} \bmod 2537=1317$ (根據第15題)

第三組 0210 密文 $C=(0210)^{13} \bmod 2537=2117$ (根據第16題)

因此 ATTACK經RSA加密後為 2299 1317 2117

18. $X\equiv 2 \pmod 3$ $a_1=2$ $m_1=3$

$X\equiv 1 \pmod 4$ $a_2=1$ $m_2=4$ $m=m_1\cdot m_2\cdot m_3=60$

$X\equiv 3 \pmod 5$ $a_3=3$ $m_3=5$

$M_1=\frac{m_1\cdot m_2\cdot m_3}{m_1}=20$ $M_2=\frac{m_1\cdot m_2\cdot m_3}{m_2}=15$ $M_3=\frac{m_1\cdot m_2\cdot m_3}{m_3}=12$

inverse $y_1$ of $M_1$ modulo $m_1=2$ $70\equiv 1 \pmod 3$

inverse $y_2$ of $M_2$ modulo $m_2=3$ $45\equiv 1 \pmod 4$

inverse $y_3$ of $M_3$ modulo $m_3=3$ $36\equiv 1 \pmod 5$

$X=a_1M_1y_1+a_2M_2y_2+a_3M_3y_3=80+45+108=233\equiv 53 \pmod{60}$