信安数基.　519021910025 王*哲.

I) 当 $x\equiv 1 \pmod{m_i}$，其它 $b_j=0$ 时，

$$x\equiv\sum_{i=1}^{k} b_i M_i' M_i \equiv b_i M_i' M_i \pmod{m}$$

$$\equiv M_i' M_i \pmod{m} \Rightarrow x = M_i' M_i + s\cdot m.$$

~~$x = s\cdot m+1$~~.

II) 当 $b_i=b_i$，$b_j\ (1\le j\le k, j\ne i)=0$ 时，

$$x=\sum_{i=1}^{k} b_i M_i M_i' = b_i M_i M_i' \pmod{m}$$

$$\Rightarrow x = b_i + s\cdot m.$$

III). $x\equiv\sum_{i=1}^{k} b_i M_i' M_i \pmod{m} \Rightarrow x=\left(\sum_{i=1}^{k} b_i M_i' M_i\right)+s\cdot m.$

~~IV) 设 $m_1=9$, $m_2=11$, $m_3=101$.~~

~~$m_1'=1$, $m_2'=1$, $m_3'=1$.~~

~~$\Rightarrow x=\sum_{i=1}^{3} b_i + s\cdot 9999$~~

设 IV) $m_1=9$，$m_2=11$，$m_3=101$，$m=m_1\cdot m_2\cdot m_3$.

计算 $b_i\equiv a^e \pmod{m_i}$ 以及 $b\equiv a^e \pmod{m}$

(1) $a=325$, $e=17$.

$325^{17}\equiv 1^{17}\equiv 1 \pmod{m_1}$

$325^{17}\equiv 6^{17}\equiv 6^{10}\cdot 6^7\equiv 6^7\equiv 8 \pmod{m_2}$

$325^{17}\equiv 22^{17}\equiv 22\cdot 484^8\equiv 22\cdot 80^8\equiv 22\cdot 1600^4\equiv 22\cdot 85^4$

$\equiv 9 \pmod{m_3}$

$$\Rightarrow a^e\equiv b \pmod{m} \Leftrightarrow \begin{cases} a^e\equiv b_1 \pmod{m_1} \\ a^e\equiv b_2 \pmod{m_2} \\ a^e\equiv b_3 \pmod{m_3}. \end{cases}$$

$$\Rightarrow b\equiv 514 \pmod{m}.$$

(ii) $a = 2325$, $e = 17$, $m_1 = 9$, $m_2 = 11$, $m_3 = 101$

$b_1 \equiv 2325^{17} \equiv 3^{17} \equiv 3^{16} \cdot 3 \equiv 9^8 \cdot 3 \equiv 0 \pmod 9$.

$b_2 \equiv 2325^{17} \equiv 4^{17} \equiv 4^{16} \cdot 4 \equiv 16^8 \cdot 4 \equiv 5^8 \cdot 4 \equiv 4 \cdot 25^4$

$\equiv 4 \cdot 3^4 \equiv 5 \pmod{m_2}$

$b_3 \equiv 2325^{17} \equiv 2^{17} \equiv 2^8 \cdot 2^8 \cdot 2 \equiv 54 \cdot 54 \cdot 2 \equiv 75 \pmod{101}$.

$\Rightarrow$ $\Rightarrow b \equiv 7650 \pmod m$

(iii) $a = 21325$, $e = 17$.

$b_1 \equiv 4^{17} \equiv 7 \pmod{m_1}$

$b_2 \equiv 7^{17} \equiv 6 \pmod{m_2}$

$b_3 \equiv 14^{17} \equiv 14 \cdot 14^{16} \equiv 14 \cdot 196^8 \equiv 14 \cdot 95^8 \equiv 6 \pmod{m_3}$.

$\Rightarrow b \equiv 7783 \pmod m$

~~(iii)~~ (iv) $a = 1325$, $e = 17$.

$b_1 \equiv 2^{17} \equiv 5 \pmod{m_1}$

$b_2 \equiv 5^{17} \equiv 3 \pmod{m_2}$

$b_3 \equiv 12^{17} \equiv 144^8 \cdot 12 \equiv 43^8 \cdot 12 \equiv 27 \pmod{m_3}$

$b \equiv 4370 \pmod m$.

(v) $a = 20210325$, $e = 17$

$b_1 \equiv 6^{17} \equiv 0 \pmod{m_1}$

$b_2 \equiv \cancel{9^{17} \equiv 9}\ 3^{17} \equiv 9 \pmod{m_2}$

$b_3 \equiv 23^{17} \equiv 45 \pmod{m_3}$.

$b \equiv 8226 \pmod m$

(vi) $\cancel{\varphi(m) = m_1 m_2 m_3 \frac{m_1 - 1}{m_1} \frac{m_2 - 1}{m_2} \frac{m_3 - 1}{m_3}} =$.

$\varphi(m) = \varphi(3) \cdot \varphi(3) \cdot \varphi(11) \cdot \varphi(101) = 2 \cdot 2 \cdot 10 \cdot 100 = 4000$

$e = 17$ 求 $e^{-1} \pmod{4000}$ $\Rightarrow e^{-1} = 2353$.

$b^d \equiv b^{2353} \pmod m$.

a 未给，无法求 b.

$$\begin{cases} x \equiv 2 & \bmod 3 \\ x \equiv 3 & \bmod 5 \\ x \equiv 2 & \bmod 7 \end{cases}$$

$$x \equiv \sum_{i=1}^{3} b_i M_i M_i' \equiv 23 \pmod{m}.$$