作业05.

1. 公钥：$B = t \times A \bmod p = (57, 3, 25, 31, 8)$.

"good job"：1100111110111111011111100100100000110101011011111100010

$S_1 = 57+3+8 = 68$ $S_2 = 57+3+25+31 = 116$

$S_3 = 57+3+25+31+8 = 124$ $S_4 = 57+25+31+8 = 121$.

$S_5 = 57+3+25 = 85$ $S_6 = 57+31 = 88$

$S_7 = 8$ $S_8 = 57+25+8 = 90$

$S_9 = 3+25+8 = 36$ $S_{10} = 124$

$S_{11} = 31$. ∴密文序列为 $(68, 116, 124, 121, 85, 88, 8, 90, 36, 124, 31)$.

2. $n = 35 = 5 \times 7$ 即 $p = 5, q = 7$. $\varphi(n) = 24$. $d \equiv e^{-1} \equiv 5 \bmod 24$

$M \equiv C^d \equiv 5 \bmod 35$

3. $p = 7, q = 17, e = 13$, $n = p \times q = 119$ $d \equiv e^{-1} \equiv 37 \bmod 96$

公钥：(e, n)，私钥：$(d, n) = (37, 119)$

$C \equiv m^e \bmod 119$ 即 $19^{13} \bmod 119$.

$13 = (1101)_2$ 由 $19^2 \equiv 4 \bmod 119$; $19^4 \equiv 16 \bmod 119$ $19^8 \equiv 18 \bmod 119$

∴ $19^{13} \equiv 19 \times 16 \times 18 \equiv 117 \bmod 119$ 即 $C = 117$.

4. 1) $p = 71, g = 7, y = 3$.

$C: (59, 57) \Leftarrow \begin{cases} C_1 \equiv g^k \equiv 59 \bmod 71. \\ C_2 \equiv M \cdot y^k \equiv 57 \bmod 71. \end{cases}$

2) 由1)得 $k = 3$ 时 $C_1 = 59$，则 $M' \cdot y^3 \equiv 29 \bmod 71$

解得 $M' = 30$. 即恢复 M 为 30.

5. 1) $G=(2,7)$. $n_A=7$. 则公钥 $P_A=n_A G=7G$

$2P$: $\lambda \equiv \frac{3x^2+1}{2y} \equiv \frac{13}{14} \equiv 13\times 4 \bmod 11 \equiv 8 \bmod 11$.

$x' \equiv \lambda^2-2x \equiv 64-4 \equiv 5 \bmod 11$. $y' \equiv \lambda(x-x')-y \equiv 2 \bmod 11$

$2P=(5,2)$.

同理得 $4P=2(2P)=(10,2)$. $6P=(4P)(2P)=(7,9)$.

$7P=P(6P)=(7,2)=P_A$

2) $C_1=kG=(8,3)$. $C_2=P_m+kP_A=(10,2)$. $C_m=\{C_1,C_2\}=\{(8,3),(10,2)\}$.

3) ① 计算 $n_A C_1$ ② $M=C_2-n_A\cdot C_1=(10,9)=P_m$.

6. 密钥生成: ① 大素数 p,q. 计算 $n=p\times q$. ② 选 e 满足 $\gcd(e,(p-1)\cdot(q-1))=1$.

③ 计算 d, 要求 $ed\equiv 1 \bmod \varphi(n)$. ④ 公钥 (n,e)

⑤ 私钥: $d_p \equiv d \bmod (p-1)$; $d_q = d \bmod (q-1)$;

$q_{inv} \equiv q^{-1} \bmod p$. $\Rightarrow (n, d, d_p, d_q, q_{inv})$.

加密: $c \equiv m^e \bmod n$.

解密: $\begin{cases} M_p \equiv C^{d_p} \bmod p \\ M_q \equiv c^{d_q} \bmod q \end{cases} \Rightarrow \begin{cases} m \equiv M_p \bmod p \\ m \equiv M_q \bmod q. \end{cases}$

解为: 令 $h \equiv q_{inv}(M_p-M_q) \bmod p$.

$m \equiv M_q + h\cdot q \bmod n$.

7. 公共: G, g.

① A: 选私钥 x_A. ② $A \underset{g^{x_B}}{\overset{g^{x_A}}{\rightleftarrows}} B$ ③ A 计算 $(g^{x_B})^{x_A}=g_A$

B: 选私钥 x_B. B 计算 $(g^{x_A})^{x_B}=g_B$

显然 $g_A=g_B$, 则公共密钥为 $Key=g^{x_A x_B}$