网络安全技术第六次作业

> 朱浩泽 1911530 计算机科学与技术

用模下指数幂的快速算法求 $101^{124} \mod 110$.

$$\begin{aligned}
a &= 101, x = 12 = 1111100, n = 110 \\
g_6 &= 101 \mod 110 = 9 \\
g_5 &= ((g_6^2 \mod 110) \cdot 101) \mod 110 = 41 \\
g_4 &= ((g_5^2 \mod 110) \cdot 101) \mod 110 = 51 \\
g_3 &= ((g_4^2 \mod 110) \cdot 101) \mod 110 = 21 \\
g_2 &= ((g_3^2 \mod 110) \cdot 101) \mod 110 = 101 \\
g_1 &= g_2^2 \mod 110 = 81 \\
g_0 &= g_1^2 \mod 110 = 71 \\
&\therefore 101^{124} \mod 110 = 71
\end{aligned}$$