and so $y = 2425$. Further, $r' = 2269 = 2048 + 128 + 64 + 16 + 8 + 4 + 1$ and

$$\begin{aligned}
&2425 \equiv -208 \pmod{2633},\\
\Rightarrow\ &2425^2 \equiv 43264 \pmod{2633} \equiv 1136 \pmod{2633},\\
\Rightarrow\ &2425^4 \equiv 1290496 \pmod{2633} \equiv 326 \pmod{2633},\\
\Rightarrow\ &2425^8 \equiv 106276 \pmod{2633} \equiv 956 \pmod{2633},\\
\Rightarrow\ &2425^{16} \equiv 913936 \pmod{2633} \equiv 285 \pmod{2633},\\
\Rightarrow\ &2425^{32} \equiv 81225 \pmod{2633} \equiv -398 \pmod{2633},\\
\Rightarrow\ &2425^{64} \equiv 158404 \pmod{2633} \equiv 424 \pmod{2633},\\
\Rightarrow\ &2425^{128} \equiv 179776 \pmod{2633} \equiv 732 \pmod{2633},\\
\Rightarrow\ &2425^{256} \equiv 535824 \pmod{2633} \equiv 1325 \pmod{2633},\\
\Rightarrow\ &2425^{512} \equiv 1755625 \pmod{2633} \equiv -586 \pmod{2633},\\
\Rightarrow\ &2425^{1024} \equiv 343396 \pmod{2633} \equiv 1106 \pmod{2633},\\
\Rightarrow\ &2425^{2048} \equiv 1223236 \pmod{2633} \equiv -1109 \pmod{2633}.
\end{aligned}$$

Hence for $y = 2425$

$$\begin{aligned}
y^{r'} = 2425^{2269} &= 2425^{2048} \cdot 2425^{128} \cdot 2425^{64} \cdot 2425^{16} \cdot 2425^{8} \cdot 2425^{4} \cdot 2425\\
&\equiv -1109 \cdot 732 \cdot 424 \cdot 285 \cdot 956 \cdot 326 \cdot -208 \pmod{2633}\\
&\equiv -824 \cdot -278 \cdot 962 \cdot -208 \pmod{2633}\\
&\equiv 1 \cdot 12 \pmod{2633}\\
&\equiv 12 \pmod{2633},
\end{aligned}$$

and so $x = 12$.

Public-Key Cryptography

So far, we have seen ciphers for which once the enciphering key is known, the deciphering key can be calculated in a short amount of time.

Suppose that we have a network of individuals, any two of whom may want to exchange secret information (for example a telex system).

To avoid having an enciphering key for every pair of individuals, each of the t individuals has an enciphering key K_i of the type specified by the cipher system and a directory of the keys $K_1, K_2, \ldots, K_t$ is published.

When anyone wants to send a message to an individual i, the letters are changed to numbers and each plaintext block x is transformed into a ciphertext block $y = \tau_i(x)$. However, only individual i knows τ_i^{-1}.

In a *public key cipher system*, τ_i^{-1} cannot be calculated from τ_i is a reasonable amount of time.

The RSA system consists of enciphering key $\{(e_i, n_i)\}_{i=1}^{t}$ such that each enciphering key (e, n) has the following properties: