Privacy of data is a major concern in today's world. One way to keep data safe is through the use of cryptography. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. One such technique is a public-key system called RSA. RSA was proposed in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman. The system is considered secure based off the supposition that the factorization of composite numbers involving large primes is both resource and time intensive.

To see the decryption process in action, consider the following key $(n, k) = (2473, 1013)$ with the encrypted form of the message called ciphertext as such:

$$0464 \quad 1472 \quad 0636 \quad 1262 \quad 111$$

The decryption process starts by using the Euclidean Algorithm to find the integer $1 < j < \phi(n)$ such that $kj \equiv 1 \pmod{\phi(n)}$.

$$1013 \cdot x + \phi(2573) \cdot y = 1$$

Which results in

$$1013 \cdot 17 + 2460 \cdot (-7) = 1$$

Hence

$$1013 \cdot 17 \equiv 1 \pmod{2573}$$

Thus, the recovery exponent, j, is 17. Using this exponent on the ciphertext blocks.

$$\begin{aligned} 0464^{17} &\equiv 1704 \pmod{2573} \\ 1472^{17} &\equiv 1511 \pmod{2573} \\ 0636^{17} &\equiv 2426 \pmod{2573} \\ 1262^{17} &\equiv 1314 \pmod{2573} \\ 2111^{17} &\equiv 2223 \pmod{2573} \end{aligned}$$

Consider the following encoding from digits to letters

$$00 = A, 01 = B, 02 = C, \cdots, 24 = Y, 25 = Z, 26 = \text{[SPACE]}$$

By splitting each resultant into digits of two, (e.g 1704 → 17 04)

$$17 \quad 04 \quad 15 \quad 11 \quad 24 \quad 26 \quad 13 \quad 14 \quad 22 \quad 23$$

Which decodes to

$$R \quad E \quad P \quad L \quad Y \quad \text{[SPACE]} \quad N \quad O \quad W \quad X$$

Cleaning this up a bit, the final decrypted message is

$$REPLY \quad NOW$$

Cryptography will continue to be a vital part of a interconnected world. RSA is just one common form of cryptography being used today. As long as we are able to keep the digit length of our encodings beyond the capabilities of current technology, RSA will be a safe approach to securing data.