QUESTION

The numbers used in a public-key cipher system are large, so computers are needed to cipher and decipher messages. Here is one based on small numbers that you can do by hand.

Let $p = 3, q = 13, e = 5$.

(i) Encode the message 'HELLO' using the public-key cipher system with numbers $n = pq$ and e.

(ii) Find an integer d such that $de \equiv 1 \bmod \phi(n)$, and hence decode your encoded message. Did you get it right?

ANSWER

(i) Using A=00, B=01,...Z=25, Hello encodes as 07 04 11 11 14. As pq=39, our blocks must all be of size 1, so to encode we must evaluate 7^5, a^5, 11^5, and 14^5 mod 35. We have

$7^2 \equiv 49 \equiv 10 \bmod 39$, so $7^5 \equiv 10.10.7 \equiv 10.70 \equiv 10.-8 \equiv -80 \equiv 37 \bmod 39$.

$4^3 \equiv 64 \equiv 25 \bmod 39$, so $4^5 \equiv 25.4.4 \equiv 100.4 \equiv -17.4 \equiv -68 \equiv 10 \bmod 39$.

$11^2 \equiv 121 \equiv 4 \bmod 39$, so $11^5 \equiv 4.4.11 \equiv 4.44 \equiv 4.5 \equiv 20 \bmod 39$.

$14^2 \equiv 196 \equiv 1 \bmod 39$, so $14^5 \equiv 1.1.14 \equiv 14 \bmod 39$

Thus HELLO encodes as 37 10 20 20 14.

(ii) $\phi(n) = 39\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{13}\right) = 39.\frac{2}{3}.\frac{12}{13} = 24$, so to find d we solve $5d \equiv 1 \bmod 24$. Multiplying by 5 reveals $d \equiv 5 \bmod 24$, so to decode we need to raise each number to the power 5 mod 39 - the rest of the checks are left to you.