Cryptography (CS402)

Sample Test 2006 Solutions

(1) By Fermat's Little Theorem $3^6 \equiv 1 \bmod 7$. Hence $3^{20} = 3^{3 \cdot 6} 3^2 \equiv 2 \bmod 7$.

(2) The encryption function is $y \equiv 5x + 1 \bmod 26$. Hence the decryption function is $x \equiv 5^{-1}(y - 1) \bmod 26$. To find $5^{-1} \bmod 26$ apply Extended Euclidean Algorithm. We obtain that $5^{-1} \equiv 21 \bmod 26$. Hence the decryption function is $x \equiv 21y + 5 \bmod 26$. Now SKPNPNBSVNS $\rightarrow$ 18 10 15 13 15 13 1 18 21 13 18 $\rightarrow$ 19 7 8 18 8 18 0 19 4 18 19 $\rightarrow$ THISISATEST.

`Answer.`THIS IS A TEST.

(3) Factorizing n we obtain that $n = 2^3 \cdot 7^2 \cdot 13$. Hence $\varphi(n) = (2^3 - 2^2)(7^2 - 7)(13 - 1) = 2016$.

(4)(i) NEW$\sqcup$Test $\rightarrow$ 13 4 22 26 19 4 18 19 $\rightarrow$ (13 4) (22 26) (19 4) (18 19) $\rightarrow$ $13 \cdot 27 + 4$ $22 \cdot 27 + 26$ $19 \cdot 27 + 4$ $18 \cdot 27 + 19$ $\rightarrow$ 355 620 517 505. Substituting these values for variable x into the encryption function $y \equiv x^3 \bmod 1189$ we obtain 372 84 455 1090. Now representing these numbers to the base 27 we have $(0 \cdot 27^2 + 13 \cdot 27 + 21)$ $(0 \cdot 27^2 + 3 \cdot 27 + 3)$ $(0 \cdot 27^2 + 16 \cdot 27 + 23)$ $(1 \cdot 27^2 + 13 \cdot 27 + 10) \rightarrow$ 0 13 21 0 3 3 0 16 23 $\rightarrow$ ANVADDAQX.

`Answer.`ANVADDAQX.

(ii) Trying primes less than $\sqrt{n}$ we obtain $n = 29 \cdot 41$. Hence $\varphi(n) = 28 \cdot 40 = 1120$, and $3^{-1} \bmod 1120$ equals 747. The decryption key is $(1189, 747)$.