Exercise (1) See the solution in tutorials.

Exercise (2)

To prove $b^{ed} \equiv b$ mod n it is enough to show that $b^{ed} \equiv b$ mod p and $b^{ed} \equiv b$ mod q. Since $ed \equiv 1 \bmod \varphi(n)$, we have that $ed = 1 + k(p-1)(q-1)$ for some integer k. Hence $b^{ed} = b^{1+k(p-1)(q-1)} = b \cdot (b^{k(p-1)})^{(q-1)} \equiv b$ mod p, because by Fermat's Little Theorem $b^{p-1} \equiv 1$ mod p. Similarly we can prove that $b^{ed} \equiv b$ mod q.

Exercise (3)

(a) Given $n = 2047$, $e = 179$, $k = 2$, $l = 3$, $N = 40$. Hence the encryption function is $y \equiv x^{179} \bmod 2047$.

SEND␣\$7500 $\longrightarrow$ 18 4 13 3 26 29 37 35 30 30 $\longrightarrow$

$18 \cdot 40 + 4 | 13 \cdot 40 + 3 | 26 \cdot 40 + 29 | 37 \cdot 40 + 35 | 30 \cdot 40 + 30 | \longrightarrow$

724 523 1069 1515 1230. Substituting these values in the encryption function for variable x we obtain 1906 1072 802 364 710.

Next we represent these numbers to the base 40 and complete the encryption process.

$40^2 + 7 \cdot 40 + 26 | 26 \cdot 40 + 32 | 20 \cdot 40 + 2 | 9 \cdot 40 + 4 | 17 \cdot 40 + 30 | \longrightarrow$

17 26 0 26 32 0 20 2 0 9 4 0 17 30 $\longrightarrow$ BH␣A␣2AUCAJEAR0.

Remark. To compute the values of the encryption function you should apply the repeated squaring method. Say, to find $y \equiv x^{179} \bmod 2047$ you should represent 179 as a base-2 number $179 = 2^7 + 2^5 + 2^4 + 2 + 1$, and $x^{179} = x^{2^7} x^{2^5} x^{2^4} x^2 x$. Now find the remainder of x mod 2047, and then the remainder of its square mod 2047, square of the square and so on till the power 2^7. The product of corresponding remainders will give you the answer.

(b) To factorize $n = 2047$ let us try various primes which are less than $\sqrt{n}$, that is less than 45. Since 23 divides n, we obtain the factorization $n = 23 \cdot 89$.

To break the cryptosystem, we should find the decryption key d which is the multiplicative inverse of e mod $\varphi(n)$. We have that $\varphi(n) = \varphi(23 \cdot 89) = 22 \cdot 88 = 1936$. Applying the Extended Euclidean Algorithm we find that $d \equiv e^{-1} \bmod 1936$ equals 446.

(c) By **(b)** we know that $n = 23 \cdot 89$. The least common multiple $l = lcm(p-1, q-1) = lcm(22, 88)$ equals 88, that is reasonable small. Therefore we can break the cryptosystem as follows. Since l divides $\varphi(n) = 22 \cdot 88$ and e is coprime to $\varphi(n)$, we have that e is coprime to l. Hence there exists a multiplicative inverse d of e mod l. Since l is small, we can repeatedly invert e mod t for increasing integer values of t, and test to see whether we have a dercryption key.

Exercise (4)

(a) Given $n = 21583$, $d = 20787$. Hence the decryption function is $x \equiv y^{20787} \bmod 21583$. Taking into account that the length of the cryptotext alphabet is 28 we obtain

YSNAUOZHXXH$\sqcup$ $\longrightarrow$ 24 18 13 0 20 14 25 7 23 23 7 26 $\longrightarrow 24 \cdot 28^2 + 18 \cdot 28 + 13|0 \cdot 28^2 + 20 \cdot 28 + 14|25 \cdot 28^2 + 7 \cdot 28 + 23|23 \cdot 28^2 + 7 \cdot 28 + 26|$ $\longrightarrow$ 19333 574 19819 18254.

Now substitute these numbers into the decryption function for the variable y, and then represent the obtained numbers as numbers to the base 27 (because the length of encryption alphabet is 27). We have

13649 11 652 660 3286 $\longrightarrow$

$17{\cdot}27^2{+}19{\cdot}27{+}14|15{\cdot}27^2{+}26{\cdot}27{+}15|0{\cdot}27^2{+}24{\cdot}27{+}12|4{\cdot}27^2{+}13{\cdot}27{+}19|$ $\longrightarrow$

18 19 14 15 26 15 0 24 12 4 13 19 $\longrightarrow$ STOP$\sqcup$PAYMENT.

(b) (i) Applying Extended Euclidean Algorithm we obtain $e \equiv 20787^{-1} \bmod 21280$ equals 6043.

(ii) We can find p, q from the following system of equations: $(p-1)(q-1) = \varphi(n)$, $pq = n$. We have $\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1$. Hence $p + q = 304$ (given $\phi(n) = 21280$ and $n = 21583$.

Then $q = 304 - p$ in $pq = 21583$ gives $p = 113$ and $q = 191$. `Answer.` $21583 = 113 \cdot 191$.