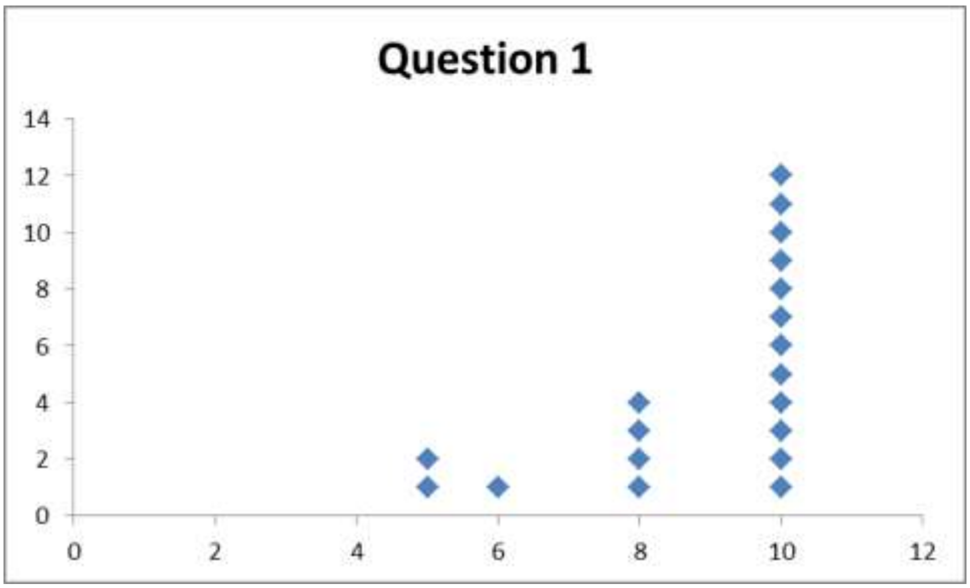
Name __Solutions____ Discrete II, Test 3, 4/21/2014

1) Determine whether or not 113 is prime in as few steps as possible. Show all your work. (10 points)

$2 \nmid 113$
$3 \nmid 113$
$5 \nmid 113$
$7 \nmid 113$

∴ 113 is prime.

(We only needed to check the primes up to $\sqrt{113} < 11$)

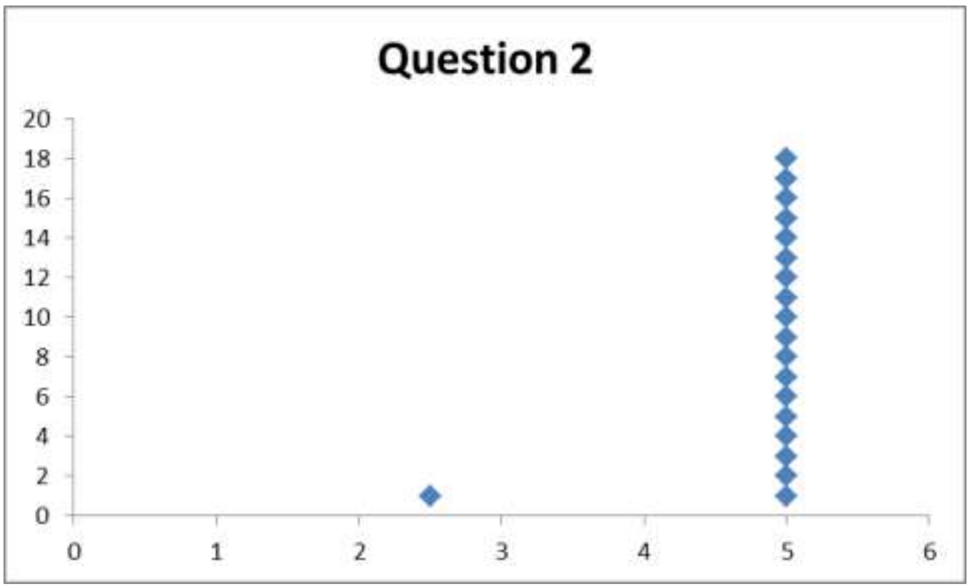


2) Find $\gcd(60,90)$. (5 points)

$$60 = 5 \cdot 3 \cdot 2^2$$
$$90 = 5 \cdot 3^2 \cdot 2$$

They have in common: $5 \cdot 3 \cdot 2 = 30$

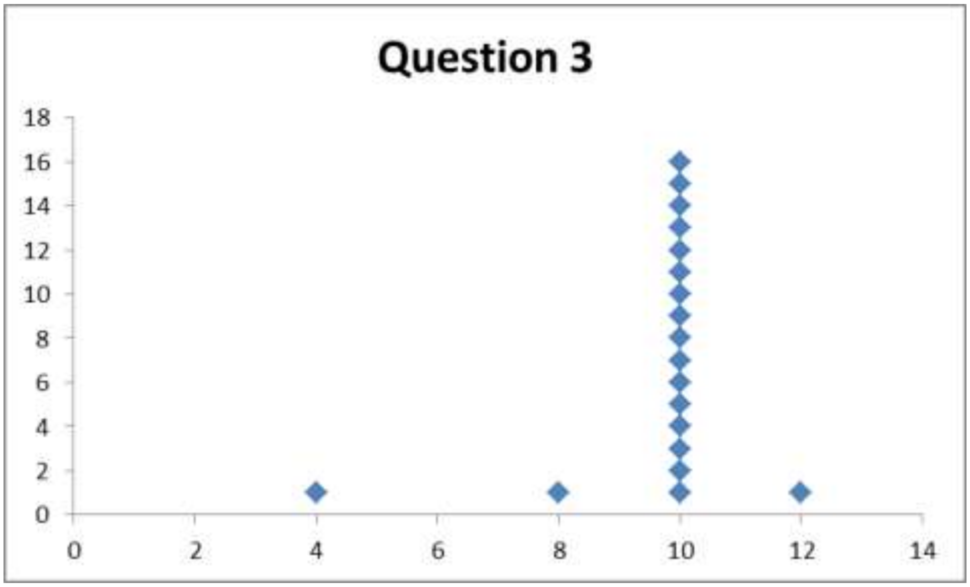
Most people used the Euclidean Algorithm, which worked too.



3) Let n, c, and d be integers. Assume that $dc|nc$. Give a brief explanation to justify why $d|n$. (10 points)

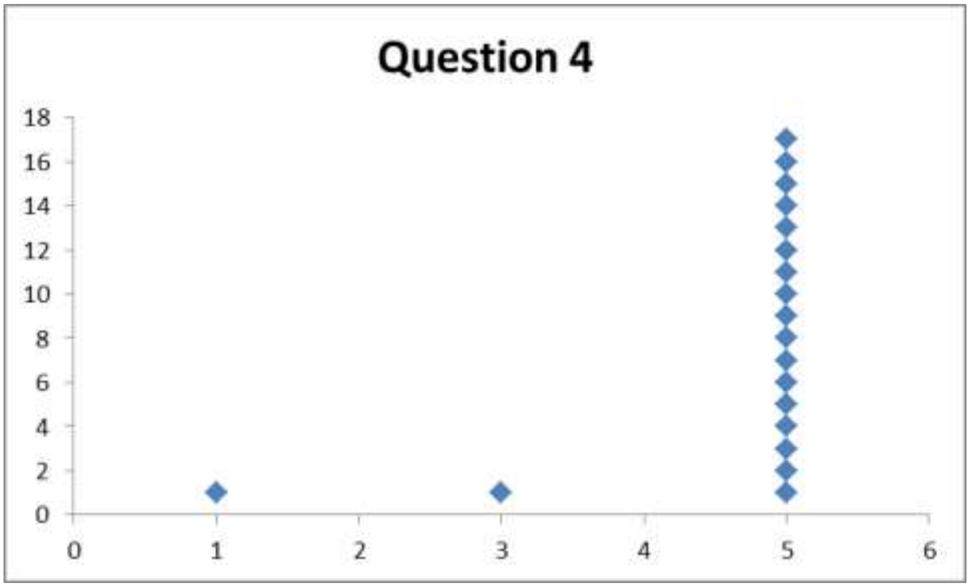
Assuming that $dc|nc$, we can write $dck = nc$ for some integer k. Canceling the $c's$ we see that $dk = n$ which says that $d|n$.

Any explanation in the right ballpark: addressing the fact that c is common to both dc and nc was given full credit.



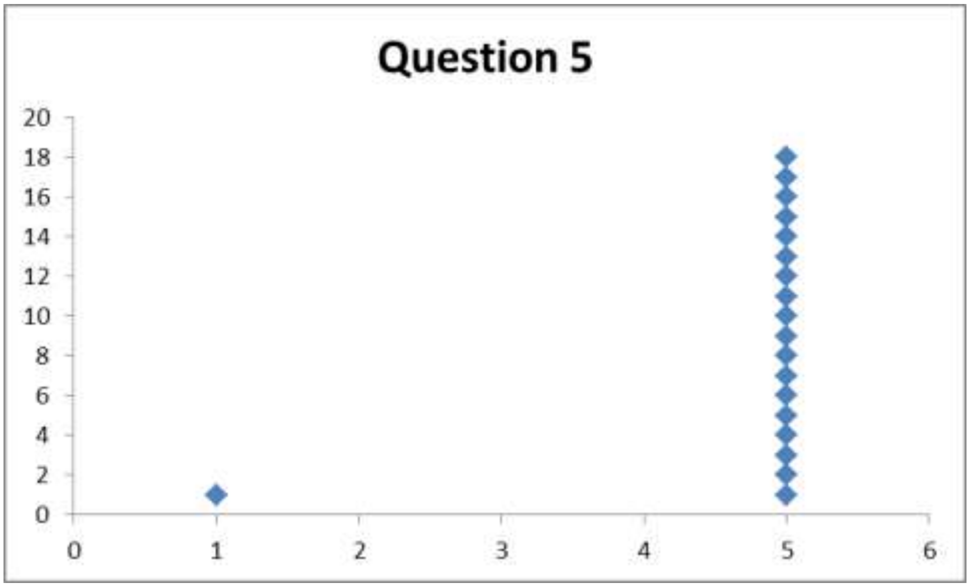
4) Find $4 + 3 \bmod 5$. (5 points)

$4 + 3 = 7 \equiv 2 \bmod 5$



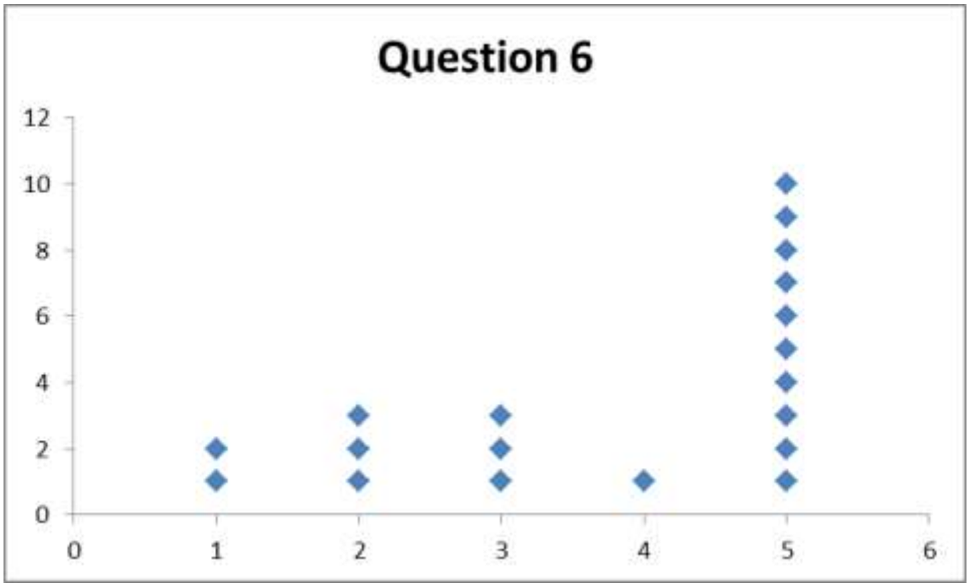
5) Find $2 \cdot 3 \bmod 5$. (5 points)

$2 \cdot 3 = 6 \equiv 1 \bmod 5$



6) Find $3 - 4 \bmod 5$. (5 points)

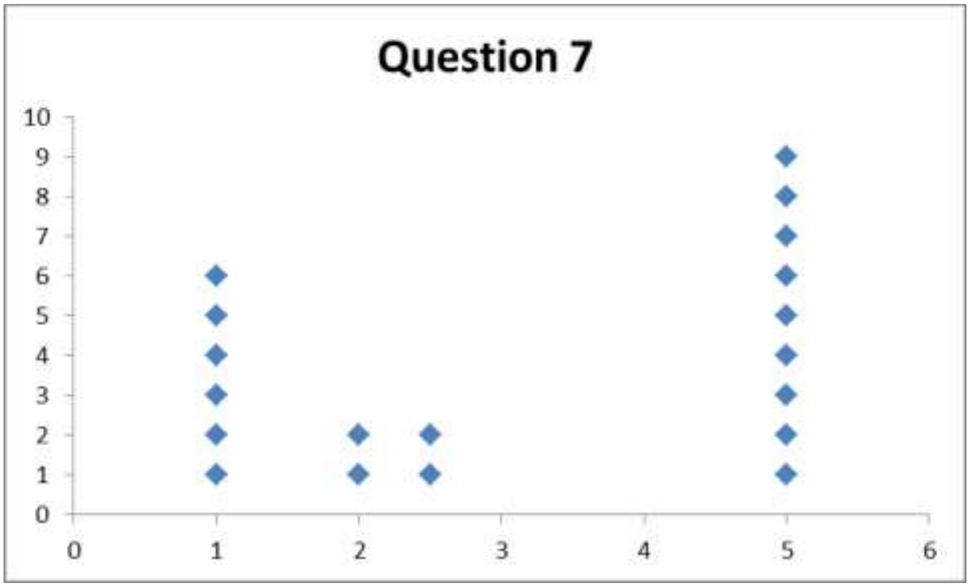
$3 - 4 = -1 \equiv 4 \bmod 5$



7) Find $4 \div 3 \bmod 5$. (5 points)

$3 \cdot 2 = 6 \equiv 1 \bmod 5$, so $3^{-1} = 2$.

$4 \div 3 \equiv 4 \cdot 2 = 8 \equiv 3 \bmod 5$



8) Find 444^{333} mod 5. (5 points)

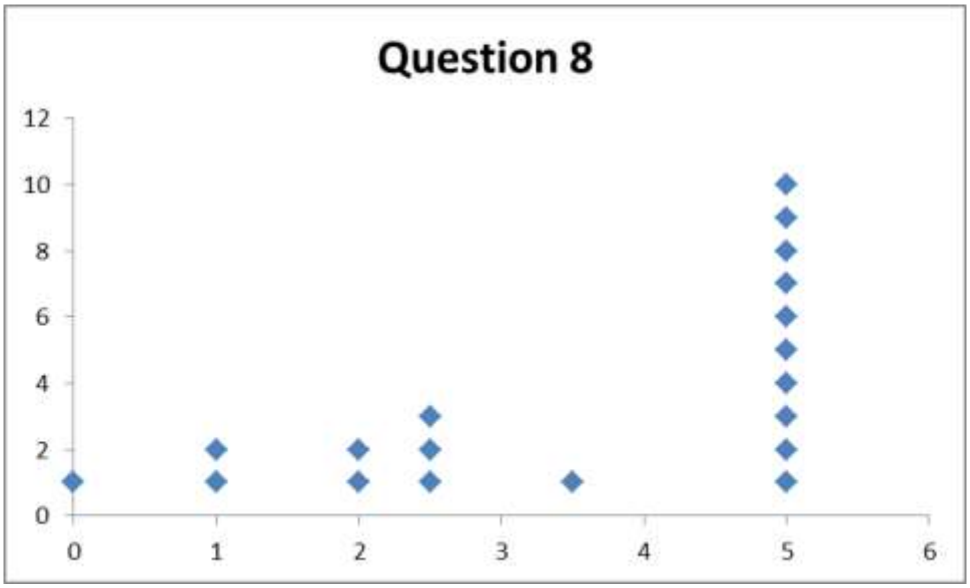
$444 \equiv 4 \bmod 5$, so this is:

$$4^{333} \bmod 5$$

5 is prime, so Fermat's little theorem tells us that $4^4 \equiv 1 \bmod 5$.

$333 = 83 \cdot 4 + 1$, so we finally have:

$$4^{333} = (4^4)^{83} \cdot 4 \equiv 1^{83} \cdot 4 \equiv 4 \bmod 5$$

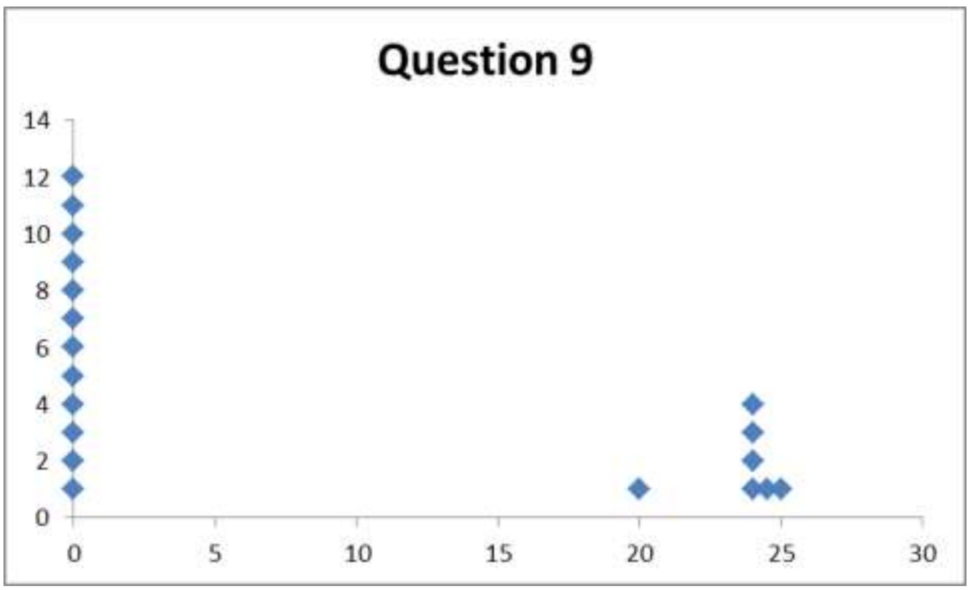


9) Find 99^{-1} mod 500. (25 points)
(Don't try to rush this problem! Take your time and write out each step)

$500 = 5 \cdot 99 + 5$ $\quad$ $5 = 500 - 5 \cdot 99 \equiv -5 \cdot 99$
$99 = 19 \cdot 5 + 4$ $\quad$ $4 = 99 - 19 \cdot 5 \equiv 99 - 19 \cdot (-5 \cdot 99) \equiv 96 \cdot 99$
$5 = 1 \cdot 4 + 1$ $\quad$ $1 = 5 - 4 \equiv -5 \cdot 99 - 96 \cdot 99 = -101 \cdot 99 = 399 \cdot 99$

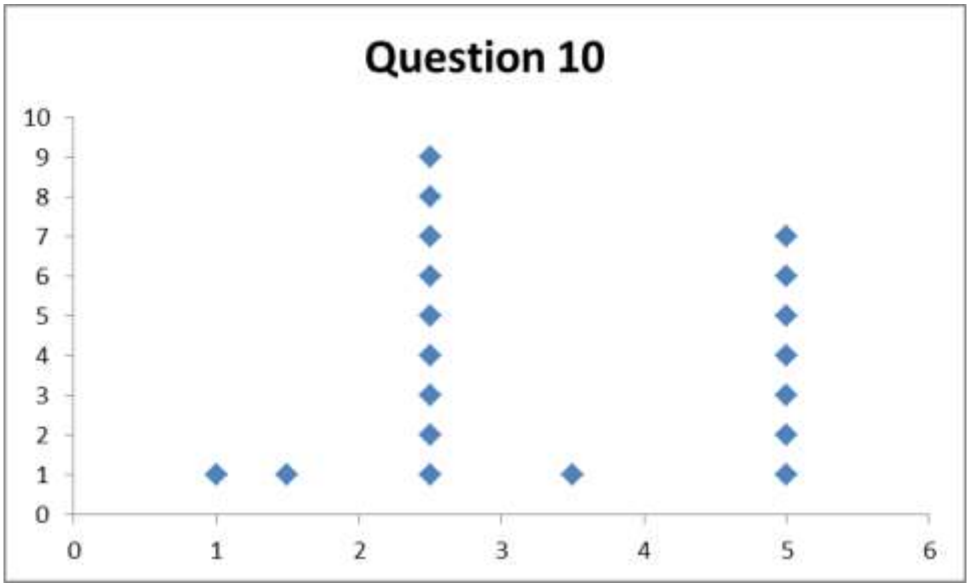
Above by decomposing 1 as $399 \cdot 99 \bmod 500$ we see that $99^{-1} = 399$.

This problem was graded in one of two ways, because I didn't want to take off two and a half letter grades if you missed this problem:
If you were on the right track, it was graded as stated, out of 25 points.
If you had essentially nothing worthwhile, it was graded as a 0 of 8.33 points. 8.33 was chosen because that makes this problem worth one letter grade. (In this case it was graded in pink instead of red)



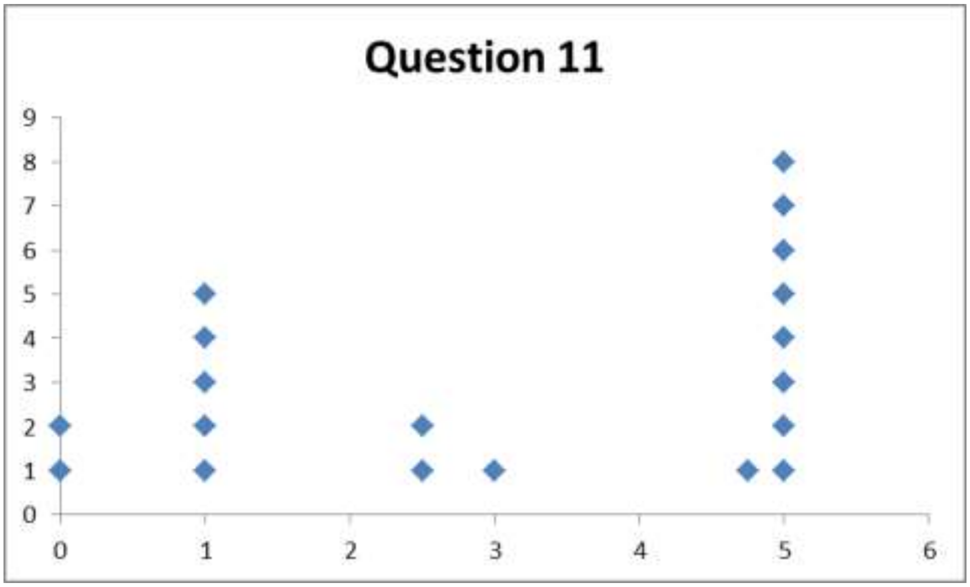
In problems 10-12, use the primes 5 and 7 to construct an RSA cryptosystem using the encryption key 11.
10) Find the modulus the communication channel should use. (5 points)

$$5 \cdot 7 = 35$$



11) Find the encryption function. (Using the key 11 as specified above) (5 points)

$$e(x) = x^{11}$$

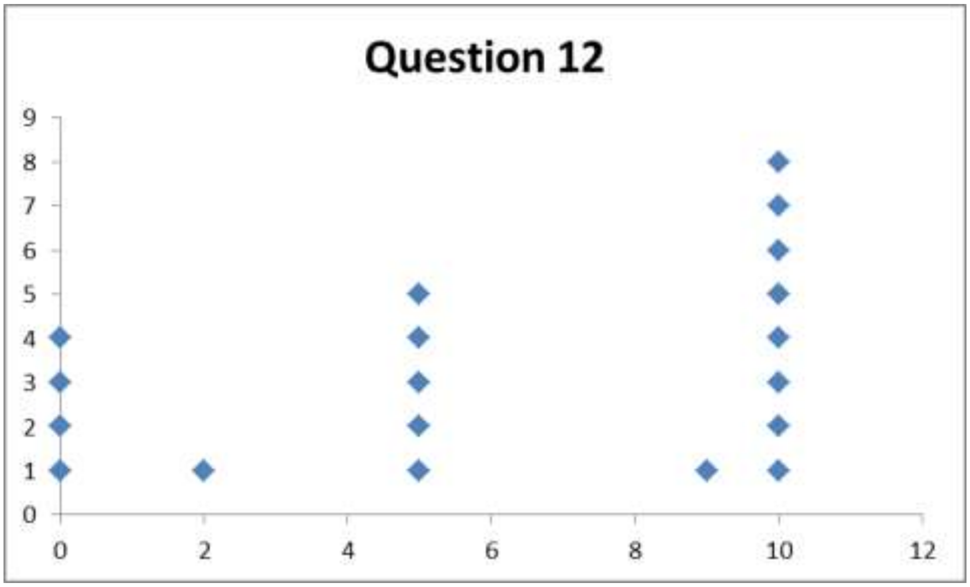


12) Find the decryption function. (Corresponding to the encryption key 11) (10 points)

We need to find 11^{-1} mod $\varphi(35) = 4 \cdot 6 = 24$. $11 \cdot 11 = 121 \equiv 1 \bmod 24$, so $11^{-1} = 11$.

Hence the decryption function is:

$$d(y) = y^{11}$$



13) Briefly explain the purpose of cryptography. (5 points)

Any answer that expressed the idea of one or more persons trying to keep information secure in the presence of a third party that may get a chance to read the information was given full credit.