Encryption

84

```
def gen (pt, key):
if    len (pt) == len (key):
          return key

else:
      key = list (key)
      for i in range (len (pt) - len (key))
          key.append (key [i % len (key)])

   return ("".join (key))

def en (pt, key):
    ct = [ ]   # Cipher text

    for i in range (len (pt)):
        x = (ord (key [i]) + ord (pt [i])) % 26
                  + ord ('A')

        ct.append (chr (x))
return    ("".join (ct)
```

```
def dec (ct, key):
    pt = []
    for i in range (len(key)):
        x = (ord(ct[i]) - ord(key[i])) % 26 + ord('A')
        pt.append(chr(x))
    return ("".join(pt))
```

Q1 $q = 17$

$p = 5$

let Alice & bob's key (Private) be x_s and x_r respectively

$x_s = 4$, $x_r = 6$

let r_s & r_r be the Public key of Alice & bob respectively

$r_s = (p)^{x_s} \% q$

$= (5)^4 \% 17$

$= 13$

$r_r = (p)^{x_r} \% q$

$= 5^6 \% 17$

$= 2$

Now r_s & r_r will be exchanged

let k_a and k_b be secret key

$k_a = (r_r)^{x_s} \% q$

$k_a = (2)^4 \% 17$

$k_a = 16$

$k_b = (r_s)^{x_r} \% q$

$= (13)^6 \% 17$

$= 16$

$\therefore k_a = k_b$