# R4, R6, R7, P1, P7, P8, P10

R4:

* If the attacker choses the decrypted version, it’s a known-plaintext. If they choose the encrypted message, it would be a chosen plain text

R6:

* Symmetric key: N(N-1)/2 pairs = N(N-1)/2 leys
* Public key: 2N keys

R7:

* A % n = 23
* B % n = 4, therefore
* (a \* b) % n = (23 \* 4) = 92

P1:

* Uasi si my cmiw lokngch
* Wasn't that fun

P7:

|  |  |  |  |
| --- | --- | --- | --- |
| letter | m | ^9 | % 33 |
| d | 4 | 262144 | 25 |
| o | 15 | 38443359375 | 3 |
| g | 7 | 40353607 | 19 |

|  |  |  |  |
| --- | --- | --- | --- |
| c | c^9 | % 33 | letter |
| 25 | 3814697265625 | 4 | d |
| 3 | 19683 | 15 | o |
| 19 | 322687697779 | 7 | g |

P8:

* A
  + N = p\*q = 55
  + Z = (p-1)(q-1) = 40
* B:
  + Doesn't factor with n, less than n
* C
  + (ed-1) / z =
  + (3\*d – 1)/40 =>
  + D = 27
* D
  + M^e = 8^3 = 512
  + C = m^e % n = 512 % 55 = 17