Eli Sabylak 3-Jan-16

Net: Ch8

R4, R6, R9, R10, P2, P8-P10

R4: You could do a cyphertext attach using the known letters of the message you had. You could probably work out the rest of the letters too.

R6: You'd need N-1 keys on the first case. In the second case you'd need N keys

R9: Hashes are completly unique in that messages A and b, Hash (H); H(a) will Never = H(b)

R10: Nothing is 100% safe, so I assume in some way one could "decrypt" a hashed message, although I'm not sure how exactly.

P2: Alice and bob together are 7 (seven) total letters. Therefore she now knows 7 of the 26 letter pairings which would be about 19 less pairing she needs to know.

P8: RSA; where $p=5$ and $q=11$

a) $N = p \cdot q$ and $z = (p-1) \cdot (q-1)$

$n = 55$

$z = 4 \cdot 10$

$z = 40$

$e < n$; no common factors

b) let $e = 3$

$d < 160$

c) $e \cdot d \bmod z = 1$ } $d \cdot e \equiv 1 \pmod{z}$

$3 \cdot d \bmod 40 = 1$ } $d \cdot 3 = 1 \pmod{40}$

81

$3 \cdot 27$ mod ~~d~~ $40 = 1$ $27 \cdot 3 = 1 \pmod{40}$

$d = 27$