Math 451

crypto

① Strings → numbers (string − 32)

numbers → strings char(nums + 32)

② replacement cypher.

a) p

b) p − 32

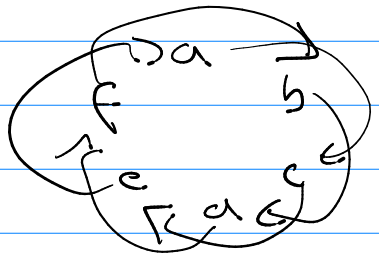
c) replacement $a \to b$ makes c
$b \to z$
⋮

d) c + 32

e) char(c+32)

③ Shift (is a replacement cypher)

ex. language



a) p

b) p − 32

c) (p − 32) + (K) shift

d) mod((p−32)+k, 95) = c

e) char(c + 32)

④ One-time-pad

a) make a string of random numbers (characters)

$p = [p_1\ p_2\ p_3\ \dots\ p_n]$

$r = [r_1\ r_2\ r_3\ \dots\ r_n]$

Same size as plain text message

b) $c_1 = \mod((p_1 - 32) + r_1, 95)$

$c_2 = \mod((p_2 - 32) + r_2, 95)$

$\vdots$

$c = [c_1\ c_2\ \dots\ c_n]$

c) $e = \text{char}(c + 32)$

Affine shift: $a(p + K) = c$

$$p = \frac{c}{a} - K$$

$\frac{1}{a} \cdot a(p+K) = c$

b/c $\frac{a}{b} = 1$ algebra

No fractions? $\mod(3(?), 11) = 1$

4c $\mod(3 \cdot 4, 11) = 1$

4 is 3's inverse mod 11

affine shift: $\text{mod}(a(p-32)+K, 95)$ encrypt

$$ap + K = c$$
$$a \cdot p = c - K$$

let $\overline{a}$ = a^{-1} inv.

$$\overline{a}\, a \cdot p = \overline{a}(c-K)$$
$$p = \overline{a}(c-K)$$

$\overline{a}$ if $\text{mod}(a, ?, 95) = 1$

Note: $\gcd(a, 95) = 1$

a) given a, K (encrypt)

$c = \text{mod}(a*(p-32)+K, 95)$

$c = \text{char}(c+32)$

b) given $\overline{a}, K$ (decrypt)

$p = \text{mod}(\overline{a}(c-K), 95)$

$m = \text{char}(p+32)$

public key crypto (RSA / Locks)

1) find p, q prime numbers (private key)

2) $n = pq$ $\quad m = (p-1)(q-1)$

3) find e a prime that has no common factors with m.

$(\gcd(e, m) = 1)$

4) find $d = \overline{e} \mod m$.

5) (private: p, q), m, n, e, (private: d) — public key (e, n)

encrypt: $c = p^e \mod n$

decrypt: $p = c^d \mod n$