Math 321

Q5 4.3 33d $\gcd(12345, 54321)$

$54321 = 4 \cdot 12345 + r_1$

$\gcd(12345, r_1)$ $12345 = 7 r_2$

(See video)

4.3 #29 prime factors

$92428 = 2 \cdot 46464$

$46464 = 2 \cdot 23232$

$23232 = 2 \cdot 11616$

$11616 = 2 \cdot 5808$

$5808 = 2 \cdot 2904$

$2904 = 2 \cdot 1452$

$1452 = 2 \cdot 726$

$726 = 2 \cdot 363$

$363 = 3 \cdot 121$

$121 = 11 \cdot 11$

$123552 \to 2^5 \cdot 3^1 \cdot 11^2 \cdot 13^0$, $2^5 \cdot 3^3 \cdot 11^1 \cdot 13^1$

(See video)

9e $\gcd(117, 213) = 3$

$3 = 5 \cdot 213 + (-9) \cdot 117$

$213 = 1 \cdot 117 + 96$

$117 = 1 \cdot 96 + 21$

$96 = 4 \cdot 21 + 12$

$21 = 1 \cdot 12 + 9$

$12 = 1 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0$

$3 = 12 - (21 - 12)$

$3 = 2 \cdot 12 - 1 \cdot 21$

$3 = 2(96 - 4 \cdot 21) - 1 \cdot 21$

$3 = 2 \cdot 96 - 9 \cdot 21$

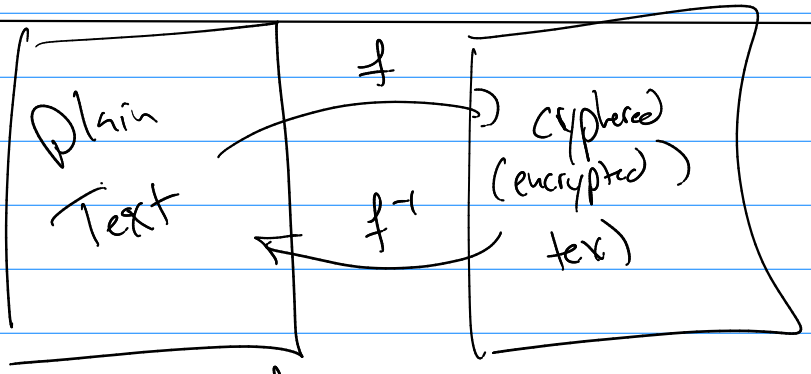
$3 = 2 \cdot 96 - 9(117 - 96)$

$3 = 11 \cdot 96 - 9 \cdot 117$

$3 = 11 \cdot (213 - 117)$ — q all 7

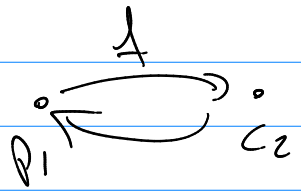
$3 = 11 \cdot 213 - 20 \cdot 117$

Cryptography



$f^{-1}(c) = p \circ \underset{f^{-1}}{\overset{f}{\rightleftarrows}} c = f(p)$

ex $p =$ idea $\underset{f^{-1}}{\overset{f}{\rightleftarrows}}$ language



symbol $\rightleftarrows$ Symbol

$p_i, c_i \in$ Alphabet

Alphabet $= \{s_1, s_2, s_3, \ldots, s_n\}$ $\quad |\#\text{alphabet}| = n$

ex Alph $= \{a, b, c, \ldots, z, w, ., ,, ', ", !, ?,$
$A, B, C, \ldots, Z\}$

---

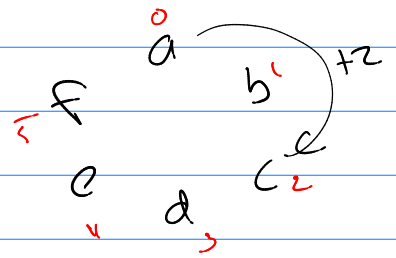
or use table to replace alphabet ex $a, b, c, d, \ldots, z$
$0, 1, 2, 3, \ldots, 25$

Private key cryptography (see video)

$n = |\text{alphabet}|$

① Shift Cypher $\quad c = (p + K) \bmod n$

$p = (c - K) \bmod n$

ex 

$c = (p+2) \bmod 7$

$p = (c-2) \bmod 7$

② Affine Shift: $\quad f(p) = (ap + K) \bmod n$

$f^{-1}(c) = (a^{-1}(c-K)) \bmod n$

a^{-1} is a's inv. mod n

ex $\quad f(p) = (3 \cdot p + 7) \bmod 11$

$f^{-1}(c) \quad (?)(c-7)) \bmod 11 = (4(c-7)) \bmod 11$

3's inv. mod 11 $\qquad 3 \cdot ? \overset{=4}{\equiv} 1 \pmod{11}$

$11 = 3 \cdot 3 + 2 \quad \rightarrow \quad 1 = 3 - 2$

$3 = 1 \cdot 2 + 1 \qquad 1 = 1 \cdot 3 - (11 - 3 \cdot 3)$

$2 = 2 \cdot 1 + 0 \qquad 1 = 4 \cdot 3 - 1 \cdot 11$

③ random replacement: (permutation)

weak to cryptanalysis

$a \leftrightarrow q$

$b \leftrightarrow M$

$c \leftrightarrow <$

$\vdots$

$z \leftrightarrow y$

(4) One-time pad

message = $p_1 p_2 p_3 \ldots p_K$

random #s = $r_1 r_2 r_3 \ldots r_K$

$C_1 = (p_1 + r_1) \bmod n$

$C_2 = (p_2 + r_2) \bmod n$

$\vdots$

$C_K = (p_K + r_K) \bmod n$