ECE 471/571 Product cipher

M S

e.g. Mult. cipher × shift cipher

$y = E_a(x) = a \cdot x \bmod 26$

$y = x + b \bmod 26$

$K = \{a \in Z_{26}, \gcd(a, 26) = 1\}$

$D_a(y) = a^{-1} \cdot y \bmod 26$

$E_{a,b}(x) = a \cdot x + b \bmod 26$

(A) Affine cipher $= M \times S$

$A' = S \times M$ (still affine)

$E_{a,b}(x) = a(x+b) \bmod 26$

$= ax + ab \bmod 26.$

M, S. (commutative)

Idempotent cryptosystem.

shift cipher $y_1 = E_{k_1}(x)$

$= x + k_1 \bmod 26$

$S \times S = ?$

$y_2 = E_{k_2}(x)$

$= x + b \bmod 26.$

$= x + k_1 + k_2 \pmod{26}$

$E_{k_1,k_2}(x) = (x + k_1) + k_2 \pmod{26}$

$= x + k_3 \pmod{26}$

still shift. cipher $\quad S \times S = S.$

S_1. $\quad S_2$. $\quad$ both

$S_1 \times S_1 = S_1 \quad S_2 \times S_2 = S_2$ idempotent

assume $\{ \quad S_1 \times S_2 = S_2 \times S_1$. Commute.

$(S_1 \times S_2) \times (S_1 \times S_2)$

$= S_1 \times S_2 \times S_2 \times S_1$

$= S_1 \times S_2 \times S_1$

$= S_1 \times S_1 \times S_2$

$= S_1 \times S_2$. idempotent

E.x. $\quad S_1$. mult. $\quad ax \pmod{26}$

$S_1 \times S_2 = S_2 \times S_1 \quad S_2$ shift. $\quad x+b \pmod{26}$

$S_1 \times S_1 = a_1 a_2 x \pmod{26}$

$S_1 \times S_2$: $y_1 = a_1 x + b_1 \mod 26$ affine

$S_1 \times S_2$: $y_2 = a_2 x + b_2 \mod 26$

$y_1 = a_2 (a_1 x + b_1) + b_2 \mod 26$

$= a_1 a_2 x + a_2 b_1 + b_2 \mod 26$

still affine cipher.