

Affine ciphers:

$$f_E(x) = ax + b$$

$$(a, b \in \mathbb{Z}_{26})$$

(a has a M.I.)

$$f_D(x) = a^{-1}x - ba^{-1} = a^{-1}(x - b)$$

Ex: Encrypt MATHS via

$$f_E(x) = 3x + 11 \quad (26)$$

$$f_D(x) = 9(x - 11)$$

$$M=13, \quad A=1, \quad T=20, \quad H=8, \quad S=19.$$

M: $f_E(13) = 3 \cdot 13 + 11 \equiv \underline{24}$

X

A: $f_E(1) = 3 \cdot 1 + 11 = \underline{14}$

N

T: $f_E(20) = 3 \cdot 20 + 11 = 71 \equiv \underline{19}$

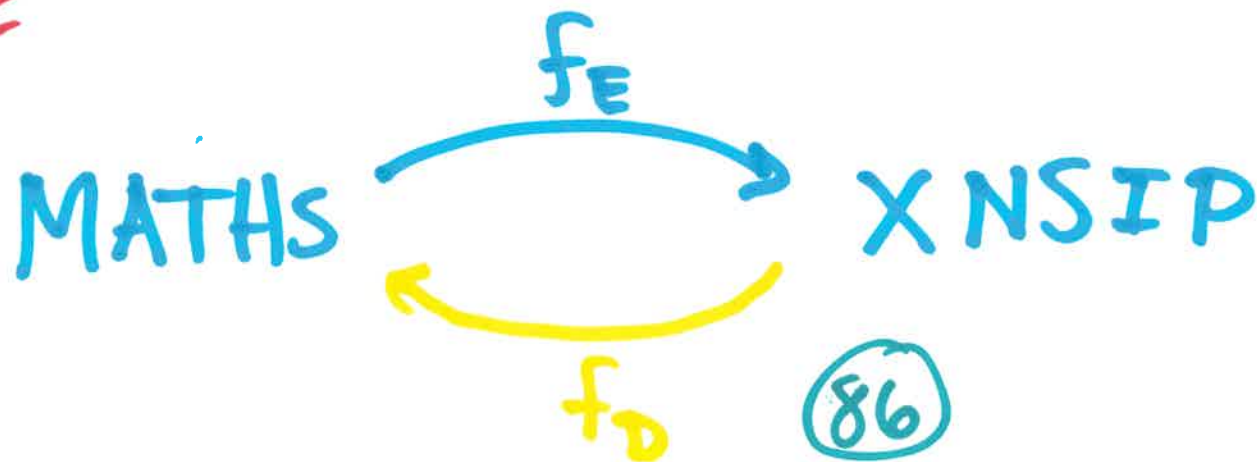
S

H: $f_E(8) = 3 \cdot 8 + 11 \equiv \underline{9}$

I

S: $f_E(19) = 3 \cdot 19 + 11 \equiv \underline{16}$

P



Ex: Same f_E (and thus f_D). Decipher

⁴
W D A Z.
²³ ¹

23	f_D	4	D
4	→	15	O
1		14	N
0		5	E

Modern crypto-system: RSA.

Rivet-Shamir-Adleman 1977.

The "tech" goes back to Euler.

RSA is a public-key crypto-system.

- public key: ~~inform~~ public information on how to encrypt.
- private key: private decipher.

Idea of RSA:

- Choose two distinct primes: p and q .
Define a composite: $N = p \cdot q$.
- Important number:

$$\varphi(N) = (p-1)(q-1)$$

- Choose an integer e such that
 $1 < e < \varphi(N)$ & $\gcd(e, \varphi(N)) = 1$.

Public-key: (N, e)

Private-key: (p, q) could include d (forthcoming)

Encrypting: Suppose x is a message to be encrypted.

$$E(x) = x^e \pmod{N}$$

Decryption:

$$\gcd(e, \varphi(N)) = 1.$$

This implies that e has a M.I. in $\mathbb{Z}_{\varphi(N)}$
so let d be in $\mathbb{Z}_{\varphi(N)}$ such that

$$e \cdot d \equiv 1 \pmod{\varphi(N)}$$

This implies that there is a k ,

$$ed = k \cdot \varphi(N) + 1.$$

$$D(y) = y^d \pmod{N}$$

(91)

Sanity check:

$$D(E(x)) = D(x^e)$$

$$= (x^e)^d$$

$$= x^{ed}$$

$$= x^{k \cdot \varphi(N) + 1}$$

Euler's Totient
Theorem

$$= \underbrace{(x^{\varphi(N)})^k}_{\equiv 1} x \pmod{N}$$

$$\equiv x \pmod{N}.$$

Studying maths

- ~~was~~ Not a good idea: just rereading notes.
- Think about sport/music/etc.
 - Need to struggle with problems.
- Have many problems on my website for you to practice.