MA190 **CRYPTOGRAPHY** – part 2, tokyo drift

Public Key cryptography → cryptosystem with the property that someone who knows only the encryption key cannot (without a prohibitively lengthy computation) discover how to decipher.

(Diffie & Hellman system 1976)
↳ Allegedly preceded by a cambridge mathematician working under secrecy → James Ellis

Affine cryptosystems are not public key.

EXAMPLE

Could be used as follows: plaintext $\xrightarrow{f_{K_E}}$ ciphertext, with $f_{K_D}^{-1}$ recovering the plaintext

K_E - enciphering key (public knowledge)
K_D - deciphering key (private)

e.g. bank communication → want to verify

to do this, the bank chooses a secret word (penis)

bank encrypts this with my public key, and emails me f_{K_E}(penis)

Using my private key, I decrypt this, and return the word

↳ I return the secret word, my identity is verified, as $f_{K_D}(f_{K_E}(\text{penis}))$ only I know K_D.

RSA PUBLIC KEY CRYPTOGRAPHY

↳ Rivest
Shamir
Adleman, 1977

- N - letter alphabet
- K - letter plaintext message units → e.g. K = 3, MEET_ME_TONIGHT
  ↳ MEE, T_M, E_T, ONI, GHT
- L - letter ciphertext message units L = 4, XAYBI243
  ↳ XAYB, I243

Plaintext message units
↳ integers in range $0 \leq i \leq N^K$

→ number of possible plaintext messages units = N^K

Ciphertext message units
↳ integers in range $0 \leq i \leq N^L$

number of possible ciphertext message units = N^L

CRYPTOSYSTEM

Each user chooses two distinct random prime numbers of around 1000 digits each. (to be safe will modern technology. ↳ $p \neq q$)
↳ choose an integer e with $\gcd(e, (p-1)) = 1$ & $\gcd(e, (q-1)) = 1$

Each user computes $n = pq$ & publishes it with the enciphering key

$$K_E = (n, e)$$

Each user computes $d = e^{-1} \bmod \varphi(n)$ $\quad (\rightarrow \varphi(n) = (p-1)(q-1))$
↳ using the euclidean algorithm

$K_D = (n, d)$ is kept secret.

The enciphering function is $\mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $x \longmapsto x^e \bmod n$
$f(n, e)$

the deciphering function is

$f(n, d)$: $\mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $x \longmapsto x^d \bmod n$

Proposition: $(x^e)^d \equiv x \bmod n$

MA149 Example of an RSA cryptosystem

N = 26 → A = 0, ..., Z = 25 26-letter alphabet, 2-letter p.n.u, 4-letter c.m.u.

K = 3

L = 4

I want to send Alice the message "YES". Her public key, found on her webpage, is $K_E^{Alice} = (46,927, 39423)$

$$YES \leftrightarrow 24 \cdot 26^2 + 4 \cdot 26^1 + 18 \cdot 26^0 = 16,346.$$

$$\oint_{(n,e)}^{Alice}(YES) = 16346^{39423} \mod 46927 \equiv 21,166 \mod 46,927$$

$21,166 \leftrightarrow$ a ciphertext unit of length 4.

$$21,166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26^1 + 2 \cdot 1$$

(How many times does it go in? — How many times does it go in? — repeat)

$= BFIC$ ← ciphertext.

It is believed that the computation of d necessitates the factorisation of n into $n = p \cdot q$

so this takes a prohibitive amount of time, with current technology