Lecture 6

RSA Public Key Cryptosystem

(Rivest, Shamir, Adelman 1977)

Suppose:

N letter alphabet (e.g. N = 26)

k-letter plaintext message units

l-letter ciphertext message units

plaintext message units $\longleftrightarrow$ integers $0 \le i \le N^k$

Ciphertext message units $\longleftrightarrow$ integers $0 \le i \le N^l$

The cryptosystem:

- Each user chooses two "random" prime numbers p, q (of around 100 digits each to be safe) plus a random integer e with $\gcd(e, p-1) = 1 = \gcd(e, q-1)$

- Each user computes $n = pq$ and publishes the enciphering key $K_E = (n, e)$.
- Each user computes (by Euclid's Algorithm)

$$d = e^{-1} \bmod \phi(n)$$

where $\phi(n) = (p-1)(q-1)$

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

- The enciphering function is

$$f_{(n,e)} : \mathbb{Z}_n \to \mathbb{Z}_n, \; x \mapsto x^e$$

Proposition

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

The deciphering function is thus

$$f_{(n,d)} : \mathbb{Z}_n \to \mathbb{Z}_n, \; x \mapsto x^d$$

It is <u>believed</u> that the computation of d necessitates the factorization of n into

$$n = pq .$$

It is <u>believed</u> that (with present methods) the factorization would take a prohibitively long time.

<u>Example</u>

26 letter alphabet ($A=0, \dots, Z=25$)

$k=3$ 3-letter plain message units

$l=4$ 4- " cipher " "

I want to send Alice the

Message

YES

Here published key is

$$K_E^{Alice} = (n, e)$$

$$= (46927, 39423)$$

$$YES \longleftrightarrow 24.26^2 + 4.26 + 18$$

$$= 16346$$

$$f_{(n,e)}(YES) \equiv 16346^{39423} \pmod{46927}$$

$$\equiv 21166$$

$$21166 = 1.26^3 + 5.26^2 + 8.26 + 2$$

$$= BFIC$$

Remark 1) Frequency analysis is no use with this cryptosystem. It can only tell us the enciphering key, which we already know.