Agenda

PROBLEM DOMAIN: NUMBER THEORY
-APPLICATION DOMAIN: CRYPTOGRAPHY
- PUBLIC KEY ENCRYPTION : RSA
DESIGN AND CORRECTNESS

Design of an Encryption Algorithm

- Requirement: A ------M-------> B
- Protocol outline:
  - Let **E(M) = M^k (mod n)** for some +ve integers n and k
  - A sends **M′ = E(M)** to B
  - B receives **M′**
  - B computes **E^{-1}(M′) = $(M')^{k'}$ (mod n)** for some +ve integer **k′**
- This requires that
  - **$M^{k*k'}$ = M (mod n)**

Ensuring Decryption Works

- For ensuring **$M^{k*k'} = M \pmod n$**:
  - we can leverage Euler's Theorem: i.e.
    - if **$k*k' = 1 + j*\phi(n)$** for some +ve integer j
      - then **$M^{k*k'} = M^{1+j*\phi(n)} = M \pmod n$**
- For ensuring **$k*k' = 1 + j*\phi(n)$** for some +ve integer **j** :
- choose **k** in **$Z^*_{\phi(n)}$** and let **k'** be inverse of **k** in ($Z^*\phi(n)$,$*\phi(n)$)
  - Then **$k*k' = 1 \pmod{\phi(n)}$** by Euler's Theorem
    - i.e. **$k*k' = 1 + j*\phi(n)$**
  - Note that
    - Inverse of **k** in **(Z_n^* , $*n$)** can be computed in polynomial time given **n** and **k** (by Aryabhatiya's algorithm)
- But there is a catch!

This is true only for M in Z^*_n !!

Design of a Public Key Encryption Algorithm

RECAP:

- We have: for **M** in Z^*_n
  - $M^{1+j*\phi(n)} = M (\mathrm{mod}\ n)$
- and by choosing **k** in $Z^*_{\phi(n)}$ and **k'** as the inverse of **k** in $(Z^*_{\phi(n)}, *_{\phi(n)})$, we have
  - $M^{k*k'} = M^{1+j*\phi(n)} = M\ (\mathrm{mod}\ n)$

Generalization

- By choosing $n = p * q$ for primes **p** and **q**, for any **M** in Z_n
  - we claim $M^{1+j*\phi(n)} = M(\mathrm{mod}\ n)$ (*see Lemma next slide*)
  - and thus $M^{k*k'} = M^{1+j*\phi(n)} = M\ (\mathrm{mod}\ n)$.

Ensuring Decryption Works for any message

- Lemma:
  - Assuming **$n = p * q$** for primes **p** and **q**, **$M^{1+j*\phi(n)} = M \pmod{n}$** for **$M$** in **$Z_n$**
- Proof:
  - If **$n = p*q$**, then **$\gcd(M,n)$** must be **1** or **p** or **q**.
    - if **$\gcd(M,n) = 1$** then **$M^{1+j*\phi(n)} = M \pmod{n}$** [by E.T]
    - if **$\gcd(M,n) = p$** then
      - **$M^{1+j*\phi(n)} = M = 0 \pmod{p}$** [by assumption]
      - **$M^{1+j*\phi(n)} = M^{1+j*\phi(p)*\phi(q)} = M \pmod{q}$** [by E.T.]
    - and therefore **$M^{1+j*\phi(n)} = M \pmod{pq}$** [since **$\gcd(p,q)=1$**]
    - if **$\gcd(M,n) = q$** then **$M^{1+j*\phi(n)} = M \pmod{pq}$** similarly.

corollary of Chinese Remainder Theorem

Encryption Algorithm - RSA

- RSA-Protocol Outline:
  - Let $\mathbf{E(M) = M^k \ (mod\ n)}$ for some $\mathbf{n = p*q}$ where **p** and **q** are primes and some **k** in $\mathbf{Z^*_{\phi(n)}}$
  - A sends $\mathbf{M' = E(M)}$ to B
  - B receives **M'**
  - B computes $\mathbf{E^{-1}(M') = (M')^{k'} \ (mod\ n)}$ where **k'** is the inverse of **k** in $(Z^*_{\phi(n)}, * \ \phi(n))$
- Communication Correctness:
  - (*see previous slides*) $\mathbf{E^{-1}(E(M)) = M}$
- Communication Efficiency:
  - *Exponentiation modulo n* can be computed in *polynomial time*