Introduction to Cryptography CS 355

Lecture 23

Attacks on RSA

Lecture Outline

- Quadratic Residues Modulo a composite number
- Attacks on RSA

Notation clarification

- $Z_n^* = \{ 0<a<n \mid \gcd(a,n)=1 \}$
- $(Z_n^*, *)$ is a group
- $| Z_n^* | = \phi(n)$
- Z_n^* is called the standard reduced set of residues modulo n

Quadratic Residues Modulo a Composite n

Definition: a is a quadratic residue modulo n ($a \in Q_n$) if $\exists$ b $\in Z_n^*$ such that $b^2 \equiv a \bmod n$, otherwise when $a \neq 0$, a is a quadratic nonresidue

Fact: $a \in Q_n^*$, where n=pq, iff. $a \in Q_p$ and $a \in Q_q$

- The "only if" direction: $b^2 \equiv a \bmod n$, then $b^2 \equiv a \bmod p$ and $b^2 \equiv a \bmod q$
- The "if" direction: If $b^2 \equiv a \bmod p$ and $c^2 \equiv a \bmod q$, then the four solutions to the four equation sets
  1. $x \equiv b \bmod p$ and $x \equiv c \bmod q$
  2. $x \equiv b \bmod p$ and $x \equiv -c \bmod q$
  3. $x \equiv -b \bmod p$ and $x \equiv c \bmod q$
  4. $x \equiv -b \bmod p$ and $x \equiv -c \bmod q$

  satisfies $x^2 \equiv a \bmod n$

For example

- Fact: if $n=pq$, then $x^2 \equiv 1 \pmod{n}$ has four solutions that are $<n$.
  - $x^2 \equiv 1 \pmod{n}$ if and only if
    both $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$
  - Two trivial solutions: 1 and n-1
    - 1 is solution to $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$
    - n-1 is solution to $x \equiv -1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
  - Two other solutions
    - solution to $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
    - solution to $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{q}$
  - E.g., $n=3\times5=15$, then $x^2 \equiv 1 \pmod{15}$ has the following solutions: 1, 4, 11, 14

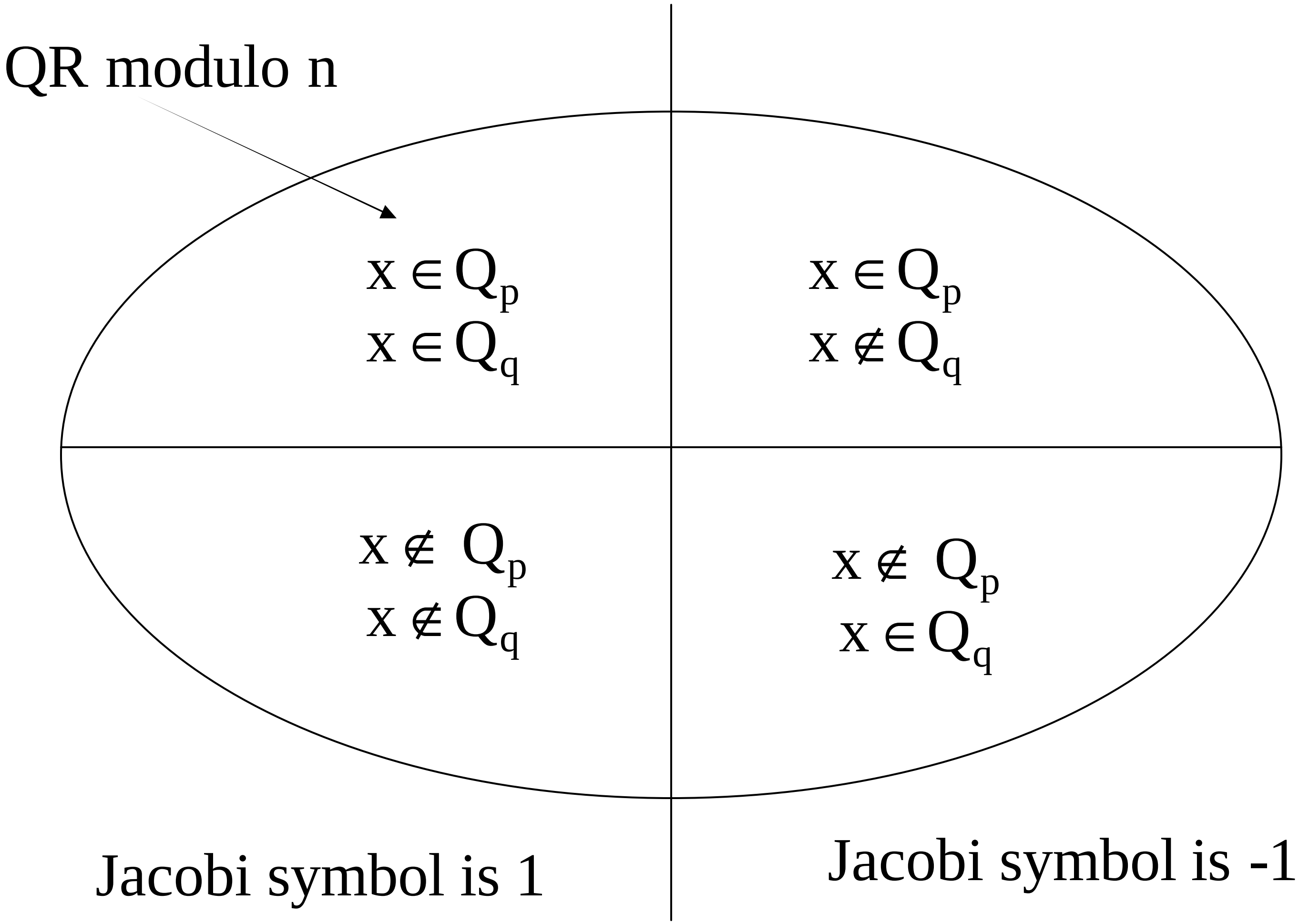
Quadratic Residues Modulo a Composite

- $|Q_n| = |Q_p| \bullet |Q_q| = (p-1)(q-1)/4$
- $\overline{Q}_n = 3(p-1)(q-1)/4$
- Jacobi symbol does not tell whether a number a is a QR

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

- when it is -1, then either $a \in Q_p \wedge a \notin Q_q$ or $a \notin Q_p \wedge a \in Q_q$, then a is not QR
- when it is 1, then either $a \in Q_p \wedge a \in Q_q$ or $a \notin Q_p \wedge a \notin Q_q$
- it is widely believed that determining QR modulo n is equivalent to factoring n, no proof is known
  - without factoring, one can guess correctly with prob. ½

Integers in Z_n*



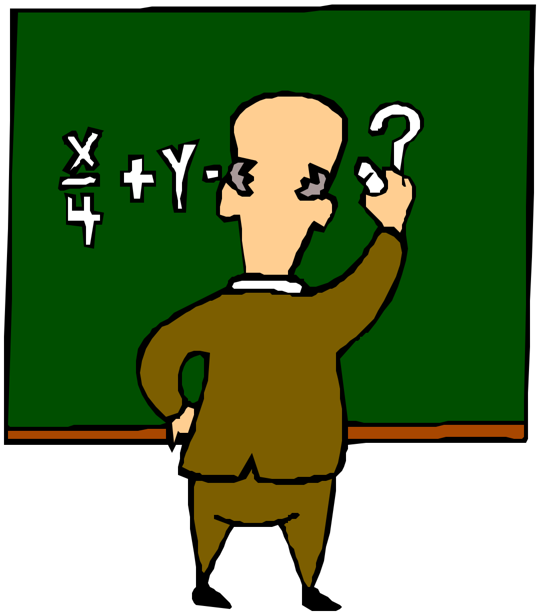
Attacks on RSA

- Goals:
  - recover secret key d
    - Brute force key search
      - infeasible
    - Timing attacks
    - Mathematical attacks
  - decrypt one message
  - learn information from the cipher texts

Math-Based Key Recovery Attacks

- Three possible approaches:
  1. Factor n = pq
  2. Determine $\Phi(n)$
  3. Find the private key d directly

- All the above are equivalent to factoring n
  - 1 implies 2
  - 2 implies 3
  - we show 2 implies 1 and 3 implies 1



Factoring Large Numbers

- Three most effective algorithms are
  - quadratic sieve
  - elliptic curve factoring algorithm
  - number field sieve
- One idea many factoring algorithms use:
  - Suppose one find $x^2 \equiv y^2 \pmod{n}$ such that $x \not\equiv y \pmod{n}$ and $x \not\equiv -y \pmod{n}$. Then $n \mid (x-y)(x+y)$. Neither $(x-y)$ or $(x+y)$ is divisible by n; thus, gcd(x-y,n) has a non-trivial factor of n

Time complexity of factoring

- quadratic sieve:
  - $O(e^{(1+o(1))\text{sqrt}(\ln n \ln \ln n)})$ for n around 2^{1024}, $O(e^{68})$
- elliptic curve factoring algorithm
  - $O(e^{(1+o(1))\text{sqrt}(2 \ln p \ln \ln p)})$, where p is the smallest prime factor
  - for n=pq and p,q around 2^{512}, for n around 2^{1024} $O(e^{65})$
- number field sieve
  - $O(e^{(1.92+o(1)) (\ln n)\text{^}1/3 (\ln \ln n)\text{^}2/3})$, for n around 2^{1024} $O(e^{60})$
- Multiple 512-bit moduli have been factored
- Extrapolating trends of factoring suggests that
  - 768-bit moduli will be factored by 2010
  - 1024-bit moduli will be factored by 2018

$\Phi(n)$ implies factorization

- Knowing both n and $\Phi(n)$, one knows

$$n = pq$$

$$\Phi(n) = (p-1)(q-1) = pq - p - q + 1$$

$$= n - p - n/p + 1$$

$$p\Phi(n) = np - p^2 - n + p$$

$$p^2 - np + \Phi(n)p - p + n = 0$$

$$p^2 + (\Phi(n) - n - 1)\, p + n = 0$$

- There are two solutions of p in the above equation, which is in standard (rather than modular) arithmetic
- Both p and q are solutions.

Factoring when knowing e and d

- Knowing ed such that $ed \equiv 1 \pmod{\Phi(n)}$

  write $ed - 1 = 2^s r$ (r odd)

  choose w at random such that $1<w<n-1$

  if w not relative prime to n then return gcd(w,n)

  (if gcd(w,n)=1, what value is ($w^{2^s r}$ mod n)?)

  compute $w^r, w^{2r}, w^{4r}, \ldots$, by successive squaring until find $w^{2^t r} \equiv 1 \pmod{n}$

  Fails when $w^r \equiv 1 \pmod{n}$ or $w^{2^t r} \equiv -1 \pmod{n}$

  Failure probability is less than ½ (Proof is complicated)

Summary of Key Recovery Math-based Attacks on RSA

- Three possible approaches:
  1. Factor n = pq
  2. Determine $\Phi(n)$
  3. Find the private key d directly
- All are equivalent
  - finding out d implies factoring n
  - if factoring is hard, so is finding out d
- Should never have different users share one common modulus
  - (why?)

Decryption attacks on RSA

- The RSA Problem: Given a positive integer n that is a product of two distinct large primes p and q, a positive integer e such that gcd(e, (p-1)(q-1))=1, and an integer c, find an integer m such that $m^e \equiv c \pmod{n}$
  - widely believed that the RSA problem is computationally equivalent to integer factorization; however, no proof is known
- The security of RSA encryption's scheme depends on the hardness of the RSA problem.

Other Decryption Attacks on RSA

Small encryption exponent e

- When e=3, Alice sends the encryption of message m to three people (public keys (e, n_1), (e, n_2), (e,n_3))
  - $C_1 = M^3 \bmod n_1$, $C_2 = M^3 \bmod n_2$, $C_3 = M^3 \bmod n_3$,
- An attacker can compute a solution to the following system

$$x \equiv c_1 \bmod n_1$$

$$x \equiv c_2 \bmod n_2$$

$$x \equiv c_3 \bmod n_3$$

- The solution x modulo $n_1 n_2 n_3$ must be M^3
  - (No modulus!), one can compute integer cubit root
- Countermeasure: padding required

Other Attacks on RSA

Forward Search Attack

- If the message space is small, the attacker can create a dictionary of encrypted messages (public key known, encrypt all possible messages and store them)
- When the attacker 'sees' a message on the network, compares the encrypted messages, so he finds out what particular message was encrypted

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

Coming Attractions …

- Discrete Log
- Diffie-Hellman
- ElGamal Encryption