Applied Cryptography and Computer Security
CSE 664 Spring 2020

Lecture 16: Second Degree Congruences and Security Applications

Department of Computer Science and Engineering
University at Buffalo

Overview

- Our coverage of public-key encryption so far included RSA and ElGamal
- Today we look at second degree congruences
  - modulo a prime
  - modulo a composite
- The security implications are:
  - ElGamal encryption needs to be modified to eliminate information leakage about encrypted plaintexts
  - factoring of an RSA modulus is possible given knowledge of e and d

Number-Theoretic Background

- Second degree congruences
  - we already learned about solving linear congruences
  - now we'll look into quadratic congruences
  - in the most general form they are $ax^2 + bx + c \equiv 0 \pmod{n}$
  - we need to learn how to take square root modulo n
  - in most cases we'll deal with congruences of the form $x^2 \equiv a \pmod{n}$
- Let's first look at the case when the modulus p is prime

Second Degree Congruences

- Solving $x^2 \equiv a \pmod{p}$ for a prime p
  - when $p = 2$, solving the congruence is easy
    - there is always one solution
    - if $a = 0$, $x \equiv 0 \pmod{2}$
    - if $a = 1$, $x \equiv 1 \pmod{2}$
  - when p is an odd prime, the congruence has solutions for some values of a and not for other values of a
    - example for $p = 11$

$$\begin{array}{rccccccccccc} x: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ x^2 \bmod 11: & 0 & 1 & 4 & 9 & 5 & 3 & 3 & 5 & 9 & 4 & 1 \end{array}$$

    - when $a = 2, 6, 7, 8, 10$, the congruence doesn't have solutions

Second Degree Congruences

- Quadratic residues
  - let n be a positive integer and a be relatively prime to n
  - a is called a quadratic residue (QR) modulo n if the congruence $x^2 \equiv a \pmod{n}$ has a solution
  - a is called a quadratic nonresidue (QNR) modulo n if the congruence $x^2 \equiv a \pmod{n}$ has no solution
  - in the example above:
    - 1, 3, 4, 5, and 9 are QRs modulo 11
    - 2, 6, 7, 8, and 10 are QNRs modulo 11
    - the class 0 is excluded from this definition

Second Degree Congruences

- Theorem: Square roots of 1 modulo p
  - if p is prime, then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$
- Theorem: Number of solutions modulo p
  - let p be an odd prime and a not be a multiple of p
  - then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or two solutions modulo p
- Theorem: Number of QRs and QNRs
  - if p is an odd prime, there are exactly $(p-1)/2$ QRs among $1, 2, \ldots, p-1$ and the same number of QNRs

Second Degree Congruences

- Legendre symbol
  - let p be an odd prime and a be an integer
  - the Legendre symbol (a/p) is defined to be $+1$ if a is a QR modulo p, -1 if a is a QNR modulo p, and 0 if p divides a
- Euler's test for a being a QR
  - let p be an odd prime and a an integer not divisible by p
  - then $a^{(p-1)/2} \bmod p$ is 1 or $p-1$
  - if it is 1, a is a QR modulo p; if it is $p-1$, a is a QNR modulo p

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Second Degree Congruences

- Properties of the Legendre symbol
  - the number of solutions to $x^2 \equiv a \pmod{p}$ is $1 + (a/p)$
  - $(a/p) \equiv a^{(p-1)/2} \pmod{p}$
  - $(ab/p) = (a/p)(b/p)$
  - if $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$
  - $(1/p) = +1$ and $(-1/p) = (-1)^{(p-1)/2}$
  - if $p \nmid a$, then $(a^2/p) = +1$ and $(a^2b/p) = (b/p)$
- Example: is 5 a QR modulo 13? how about $5 \cdot 2$?
- Let's see what implications this has on ElGamal encryption

Security of ElGamal Encryption

- Care must be taken when mapping messages to group elements
  - one (least significant) bit of discrete logarithm is easy to compute for elements of $\mathbb{Z}_p^*$
  - given a ciphertext, an adversary can tell whether the underlying plaintext was a QR modulo p or not
  - this gives the adversary an easy way to win the indistinguishability game
  - to ensure indistinguishability, we need to make sure that all values we use will have the same value for that bit
  - thus, we encode messages as $x^2 \bmod p$ only

ElGamal Encryption

- Encryption with ElGamal becomes
  - given a message m, interpret it as a integer between 1 and q, where $q = (p-1)/2$
  - compute $\hat{m} = m^2 \bmod p$ and encrypt $\hat{m}$
  - upon decryption:
    - obtain $\hat{m}$
    - compute square roots m_1, m_2 of $\hat{m}$ modulo p
    - set m to the unique $1 \le m_i \le q$
- There are alternative ways of achieving the same goal
  - e.g., setup encryption over a subgroup of $\mathbb{Z}_p^*$ of prime order q, where $p = 2q + 1$

Second Degree Congruences

- The Jacobi symbol (for composite moduli)
  - let n be an integer with prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$
  - the Jacobi symbol (a/n) is defined as

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

    where (a/p_i) are Legendre symbols

- If $gcd(a, n) > 1$, then some prime factor p of n divides $a \Rightarrow (a/p) = 0 \Rightarrow (a/n) = 0$

- Example: compute the Jacobi symbol of 3 modulo 70
  - $\left(\frac{3}{70}\right) = \left(\frac{3}{2}\right)\left(\frac{3}{5}\right)\left(\frac{3}{7}\right)$

Second Degree Congruences

- The Jacobi symbol shares many properties with the Legendre symbol
- Properties of the Jacobi symbol
  - if $a \equiv b \pmod{n}$, then $(a/n) = (b/n)$
  - $(ab/n) = (a/n)(b/n)$
  - $(a/nn') = (a/n)(a/n')$
  - if $gcd(a, n) = 1$, then $(a^2/n) = (a/n^2) = +1$, $(a^2b/n) = (b/n)$ and $(a/(n^2n')) = (a/n')$
- There are also properties with respect to $(-1/n)$, $(2/n)$ and other values

Solving Second Degree Congruences

- We know how to decide whether $x^2 \equiv a \pmod{n}$ has solutions, but how about finding them?

- Theorem
  - if $p \equiv 3 \pmod{4}$ is prime and a is a QR modulo p, then the solutions to $x^2 \equiv a \pmod{p}$ are $x \equiv \pm(a^{(p+1)/4}) \pmod{p}$
  - primes $p \equiv 3 \pmod{4}$ are called Blum primes

- Theorem
  - if $p \equiv 5 \pmod{8}$ is prime and a is a QR modulo p, then the solutions to $x^2 \equiv a \pmod{p}$ are $\pm x$, where x is computed as:

$$x \equiv a^{(p+3)/8} \pmod{p}$$
$$\text{if } (x^2 \not\equiv a \pmod{p})\ x = x2^{(p-1)/4} \bmod p$$

Solving Second Degree Congruences

- Example: solve $x^2 \equiv 6 \pmod{47}$
  - first compute $(6/47) = +1$, so 6 is a QR modulo 47
  - because $47 \equiv 3 \pmod{4}$,
    $x \equiv \pm 6^{(47+1)/4} \equiv \pm 6^{12} \equiv \pm 37 \pmod{47}$
- Theorem: square roots modulo pq
  - let p and q be distinct odd primes and a be a QR modulo pq
  - then there are exactly 4 solutions to $x^2 \equiv a \pmod{pq}$
  - there are 2 solutions to $x^2 \equiv a \pmod{p}$ and $x^2 \equiv a \pmod{q}$ each
  - when we combine them using the CRT, we obtain 4 solutions

Attacks on RSA

- We can also factor n if e and d are known

- We first look at the fact that if $n = pq$ then $x^2 \equiv 1 \pmod{n}$ has 4 solutions $< n$
  - $x^2 \equiv 1 \pmod{n}$ iff both $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$
  - two trivial solutions 1 and $n - 1$
    - 1 is the solution when $x \equiv 1 \pmod{p}$ and $x \equiv 1 \pmod{q}$
    - $n - 1$ is the solution when $x \equiv -1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
  - two other solutions
    - a solution when $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{q}$
    - a solution when $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{q}$

Attacks on RSA

- Fact: if $n = pq$ then $x^2 \equiv 1 \pmod{n}$ has 4 solutions
  - example: $n = 3 \cdot 5 = 15$
    - $x^2 \equiv 1 \pmod{15}$ has solutions 1, 4, 11, 14
  - knowing a non-trivial solution to $x^2 \equiv 1 \pmod{n}$, compute $gcd(x + 1, n)$ and $gcd(x - 1, n)$
    - they will give factors p and q
  - example: 4 and 11 are solutions to $x^2 \equiv 1 \pmod{15}$
    - $gcd(4 + 1, 15) = 5$; $gcd(4 - 1, 15) = 3$
    - $gcd(11 + 1, 15) = 3$; $gcd(11 - 1, 15) = 5$

Attacks on RSA

- Now assume that we know e and d such that $ed \equiv 1 \pmod{\phi(n)}$
- To factor n using this knowledge:
  - write $ed - 1 = 2^s r$ where r is odd
  - choose w at random such that $1 < w < n - 1$
  - if w is not relatively prime to n, return $gcd(w, n)$
  - otherwise notice that $w^{2^s r} \equiv w^{1-1} \equiv 1 \pmod{n}$
  - compute $w^r, w^{2r}, w^{2^2 r}, \ldots$ until we find $w^{2^t r} \equiv 1 \pmod{n}$
  - $w^{2^{t-1} r}$ is then a non-trivial solution to the equation which gives factorization of n
  - if $w^r \equiv 1 \pmod{n}$ or $w^{2^t r} \equiv -1 \pmod{n}$, try a different w

Attacks on RSA

- Example of factoring n when e and d are known
  - we are given $n = 2773$, $e = 17$, and $d = 157$
  - compute $ed - 1 = 2668 = 2^2 \cdot 667 \;\Rightarrow\; r = 667$
  - pick a random w and compute $w^r \bmod n$
    - $w = 7, 7^{667} \bmod 2773 = 1$, discard
    - $w = 8, 8^{667} \bmod 2773 = 471$,
      $w^{2r} \bmod n = 471^2 \bmod 2773 = 1 \;\Rightarrow\; 471$ is a non-trivial square root of $1 \bmod 2773$
    - now compute $gcd(471 + 1, 2773) = 59$ and $gcd(471 - 1, 2773) = 47$
    - thus $p = 59$ and $q = 47$

Summary

- Second degree congruences are among many number theoretic results discovered over time
- Their knowledge leads to attacks on public-key encryption and other schemes
- Awareness of such attacks is needed for secure implementation of respective algorithms