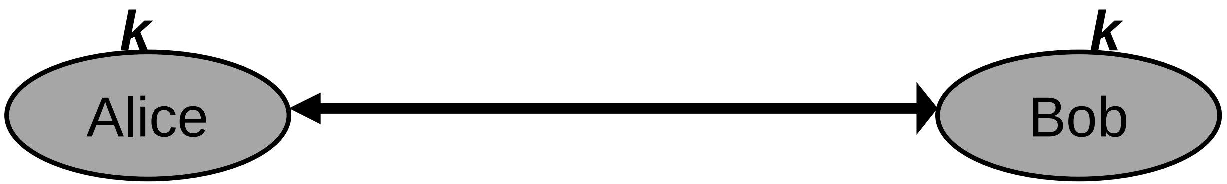
Introduction to Cryptography

Lecture 7

Benny Pinkas

Classical symmetric ciphers

- Alice and Bob share a private key *k.*
- System is secure as long as *k* is secret.
- Major problem: generating and distributing *k.*



Diffie and Hellman: “New Directions in Cryptography”, 1976.

- “We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing…

  …such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution…

  …theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.”

Diffie-Hellman

- Came up with the idea of public key cryptography

Everyone can learn Bob’s public key and encrypt messages to Bob.
Only Bob knows the decryption key and can decrypt.

Key distribution is greatly simplified.

Plan

- Basic number theory
  - Divisors, modular arithmetic
  - The GCD algorithm
  - Groups

- References:
  - Many books on number theory
  - Almost all books on cryptography
  - Cormen, Leiserson, Rivest, (Stein), “Introduction to Algorithms”, chapter on Number-Theoretic Algorithms.

Divisors, prime numbers

- We work over the integers
- A non-zero integer *b* divides an integer *a* if there exists an integer *c* s.t. $a=c\cdot b$.
  - Denoted as $b|a$
  - I.e. *b* divides *a* with no remainder
- Examples
  - Trivial divisors: $1|a$, $a|a$
  - Each of {1,2,3,4,6,8,12,24} divides 24
  - 5 does not divide 24
- Prime numbers
  - An integer *a* is prime if it is only divisible by 1 and by itself.
  - 23 is prime, 24 is not.

Modular Arithmetic

- Modular operator:
  - *a* mod *b*, (or *a%b*) is the remainder of *a* when divided by *b*
  - I.e., the smallest $r \geq 0$ s.t. $\exists$ integer *q* for which $a = qb+r$.
  - (Thm: there is a single choice for such *q,r*)

  - Examples
    - *12 mod 5 = 2*
    - 10 mod 5 = 0
    - -5 mod 5 = 0
    - -1 mod 5 = 4

Modular congruency

- a is congruent to b modulo n ($a \equiv b \bmod n$) if
  - $(a-b) = 0 \bmod n$
  - Namely, n divides $a-b$
  - In other words, $(a \bmod n) = (b \bmod n)$

- E.g.,
  - $23 \equiv 12 \bmod 11$
  - $4 \equiv -1 \bmod 5$

- There are n equivalence classes modulo n
  - $[3]_7 = \{\ldots,-11,-4,3,10,17,\ldots\}$

Greatest Common Divisor (GCD)

- d is a common divisor of a and b, if $d|a$ and $d|b$.
- $gcd(a,b)$ (Greatest Common Divisor), is the largest integer that divides both a and b. $(a,b >= 0)$
  - $gcd(a,b)$ = max k *s.t.* $k|a$ and $k|b$.

- Examples:
  - gcd(30,24) = 6
  - gcd(30,23) = 1

- If $gcd(a,b)=1$ then a and b are denoted relatively prime.

Facts about the GCD

- *gcd(a,b)* = *gcd(b, a* mod *b)* (interesting when a>b)
- Since (e.g., a=33, b=15)
  - If *c*|*a and c*|*b* then *c*|*(a mod b)*
  - If *c*|*b* and *c*|*(a mod b)* then *c*|*a*

- If *a* mod *b* = 0, then gcd(a,b)=b.

- Therefore,

gcd(19,8) =

gcd(8, 3) =

gcd(3,2) =

gcd(2,1) = 1

gcd(20,8) =

gcd(8, 4) = 4

Euclid's algorithm

Input: a>b>0

Output: gcd(a,b)

Algorithm:

1. if (*a mod b) = 0* return (*b*)
2. else return(gcd(*b, a* mod *b*))

Complexity:

- O(log *a*) rounds
- Each round requires O($\log^2 a$) bit operations
- Actually, the total overhead can be shown to be O($\log^2 a$)

The extended gcd algorithm

Finding *s, t* such that $gcd(a,b) = a \cdot s + b \cdot t$

```
Extended-gcd(a,b)  /* output is (gcd(a,b), s, t)
  1. If (a mod b=0) then return(b,0,1)
  2. (d',s',t') = Extended-gcd(b, a mod b)
  3. (d,s,t) = (d', t', s'-⌊a/b⌋·t')
  4. return(d,s,t)
```

Note that the overhead is as in the basic GCD algorithm

- Extended gcd algorithm
  - Given a,b finds s,t such that gcd(a,b) = a·s + b·t
  - In particular, if p is prime than gcd(a,p)=1, and therefore a·s+p·t=1.

- Extended gcd algorithm
  - Given a,b finds s,t such that $gcd(a,b) = a \cdot s + b \cdot t$
  - In particular, if p is prime than gcd(a,p)=1, and therefore $a \cdot s+p \cdot t=1$. This implies that ($a \cdot s \equiv 1 \bmod p$)
- THM: There is no integer smaller than gcd(a,b) which can be represented as a linear combination of a,b.
  - For example, a=12, b=8.
  - $4= 1 \cdot 12 - 1 \cdot 8$
  - There are no s,t for which $2=s \cdot 12 + t \cdot 8$
- Therefore if we find s,t such that as+tb=1, then we know that gcd(a,b)=1

Groups

- Definition: a set G with a binary operation $\circ: G \times G \to G$ is called a group if:
  - (closure) $\forall a,b \in G$, it holds that $a \circ b \in G$.
  - (associativity) $\forall a,b,c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.
  - (identity element) $\exists e \in G$, s.t. $\forall a \in G$ it holds that $a \circ e = a$.
  - (inverse element) $\forall a \in G\ \exists a^{-1} \in G$, s.t. $a \circ a^{-1} = e$.
- A group is Abelian (commutative) if $\forall a,b \in G$, it holds that $a \circ b = b \circ a$.

- Examples:
  - Integers under addition
    - (Z,+) = {…,-3,-2,-1,0,1,2,3,…}

More examples of groups

- Addition modulo N
  - $(G, \circ) = (\{0,1,2,\ldots,N-1\}, +)$

- Z_p^* Multiplication modulo a prime number p
  - $(G, \circ) = (\{1,2,\ldots,p-1\}, \times)$
  - E.g., $Z_7^* = (\{1,2,3,4,5,6\} , \times)$

- Trivial: closure (the result of the multiplication is never divisible by p), associativity, existence of identity element.
- The extended GCD algorithm shows that an inverse always exists:
  - $s \cdot a + t \cdot p = 1 \Rightarrow s \cdot a = 1 - t \cdot p \Rightarrow s \cdot a \equiv 1 \bmod p$

More examples of groups

- Z_N^* Multiplication modulo a composite number N
  - $(G, \circ) = (\{a \text{ s.t. } 1 \leq a \leq N\text{-}1$ and $gcd(a,N)=1\}, \times)$
  - E.g., $Z_{10}^* = (\{1,3,7,9\}, \times)$

  - Closure:
    - $s \cdot a+t \cdot N = 1$
    - $s' \cdot b+t' \cdot N = 1$
    - $ss' \cdot (ab)+(sat'+s'bt+ tt'N) \cdot N = 1$
    - Therefore $1=gcd(ab,N)$.
  - Associativity: trivial
  - Existence of identity element: 1.
  - Inverse element: as in Z_p^*

Subgroups

- Let $(G, \circ)$ be a group.
  - $(H, \circ)$ is a subgroup of G if
    - $(H, \circ)$ is a group
    - $H \subseteq G$
  - For example, $H = (\{1,2,4\}, \times)$ is a subgroup of Z_7^*.

- *Lagrange's theorem:*

  If $(G, \circ)$ is finite and $(H, \circ)$ is a subgroup of $(G, \circ)$, then $|H|$ divides $|G|$

  In our example: 3|6.

Cyclic Groups

- Exponentiation is repeated application of $\circ$
  - $a^3 = a \circ a \circ a.$
  - $a^0 = 1.$
  - $a^{-x} = (a^{-1})^x$
- A group G is cyclic if there exists a generator g, s.t. $\forall a \in G, \exists i$ s.t. $g^i = a$.
  - I.e., G= <g> = $\{1, g, g^2, g^3, \ldots\}$
  - For example $Z_7^* = \langle 3 \rangle = \{1,3,2,6,4,5\}$
- Not all $a \in G$ are generators of G, but they all generate a subgroup of G.
  - E.g. 2 is not a generator of Z_7^*
- The order of a group element a is the smallest $j>0$ s.t. $a^j=1$
- *Lagrange's theorem* $\Rightarrow$ for $x \in Z_p^*$, $ord(x) \mid p-1$.

Fermat's theorem

- Corollary of Lagrange's theorem: if $(G, \circ)$ is a finite group, then $\forall a \in G,\ a^{|G|}=1.$
- Corollary (Fermat's theorem): $\forall\, a \in Z_p^*,\ a^{p-1} = 1$ mod $p.$ E.g., for all $\forall a \in Z_7^*,\ a^6=1,\ a^7=a.$
- Computing inverses:
- Given $a \in G,$ how to compute $a^{-1}?$
  – Fermat's theorem: $a^{-1} = a^{|G|-1}$ $(= a^{p-2}$ in $Z_p^*)$
  – Or, using the extended gcd algorithm (for Z_p^* or Z_N^*):
    - $gcd(a,p) = 1$
    - $s \cdot a + t \cdot p = 1 \Rightarrow s \cdot a = -t \cdot p + 1 \Rightarrow$ s is a^{-1} !!
  – Which is more efficient?

Computing in Z_p^*

- P is a huge prime (1024 bits)
- Easy tasks (measured in bit operations):
  - Adding in O(log p) (namely, linear n the length of p)
  - Multiplying in O($\log^2$ p)   (and even in O($\log^{1.7}$ p))
  - Inverting (*a* to a^{-1}) in O($\log^2$ p)
  - Exponentiations:
    - x^r mod *p* in O(log r · $\log^2$ p), using repeated squaring

Groups we will use

- Z_p^* Multiplication modulo a prime number p
  - $(G, \circ) = (\{1,2,\ldots,p-1\}, \times)$
  - E.g., $Z_7^* = (\{1,2,3,4,5,6\}, \times)$
- Z_N^* Multiplication modulo a composite number N
  - $(G, \circ) = (\{a$ s.t. $1 \le a \le N-1$ and $gcd(a,N)=1\}, \times)$
  - E.g., $Z_{10}^* = (\{1,3,7,9\}, \times)$

Euler's phi function

- Lagrange's Theorem: $\forall a$ in a finite group G, $a^{|G|}=1.$
- Euler's phi function (aka, Euler's totient function),
  - $\phi(n)$ = number of elements in Z^*_n (i.e. $| \{x \mid gcd(x,n)=1, 1\leq x\leq n\} |$
  - $\phi(p) = p-1$ for a prime $p.$
  - $n=\prod_{i=1..k} p_i^{e(i)} \Rightarrow \phi(n) = n\cdot\prod_{i=1..k} (1-1/p_i)$
  - $\phi(p^2) = p(p-1)$ for a prime $p.$
  - $n=p\cdot q \Rightarrow \phi(n) =(p-1)(q-1)$

- Corollary: For Z_n^* ($n=p\cdot q$), $|Z_n^*|= \phi(n) =(p-1)(q-1).$
- $\forall a \in Z_n^*$ it holds that $a^{\phi(n)} =1$ mod n
  - For Z_p^* (prime p), $a^{p-1} =1$ mod p (Fermat's theorem).
  - For Z_n^* ($n=p\cdot q$), $a^{(p-1)(q-1)} =1$ mod n

Quadratic Residues

- The square root of $x \in Z_p^*$ is $y \in Z_p^*$ s.t. $y^2 = x \bmod p$.
- Examples: sqrt(2) mod 7 = 3, sqrt(3) mod 7 doesn't exist.
- How many square roots does $x \in Z_p^*$ have?
  - If a and b are square roots of x, then $x = a^2 = b^2 \bmod p$. Therefore $(a-b)(a+b) = 0 \bmod p$. Therefore either $a = b$ or $a = -b$ modulo p.
  - Therefore x has either 2 or 0 square roots, and is denoted as a Quadratic Residue (QR) or Non Quadratic Residue (NQR), respectively. There are exactly $(p-1)/2$ QRs.
- $x^{(p-1)/2}$ is either 1 or -1 in Z_p^*. (indeed, $(x^{(p-1)/2})^2$ is always 1)
- Euler's theorem: $x \in Z_p^*$ is a QR iff $x^{(p-1)/2} = 1 \bmod p$.
- *Legendre's symbol:*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ is a QR in } Z_p^* \\ -1 & x \text{ is an NQR in } Z_p^* \\ 0 & x = 0 \bmod p \end{cases}$$

- Legendre's symbol can be efficiently computed as $x^{(p-1)/2} \bmod p$.
- The quadratic residues form a subgroup of order $(p-1)/2$ $(=q)$

Does the DDH assumption hold in Z_p^*?

- The DDH assumption does not hold in Z_p^*
  - Assume that both $x=g^a$ and $y=g^b$ are QRs in Z_p^*.
  - Then g^{ab} is also a QR, whereas a random g^c is an NQR with probability ½.
- Solution: (work in a subgroup of prime order)
  - Set $p=2q+1$, where q is prime.
  - $\phi(Z_p^*) = p-1 = 2q$. Therefore Z_p^* has a subgroup H of *prime* order q.
  - Let g be a generator of H *(for example, g is a QR in Z_p^*).*
  - The DDH assumption is believed to hold in *H.* (The Legendre symbol is always 1.)