CS 6160 Cryptology Lecture 14 a: Introduction to Number Theory

Maria Francis

October 27, 2020

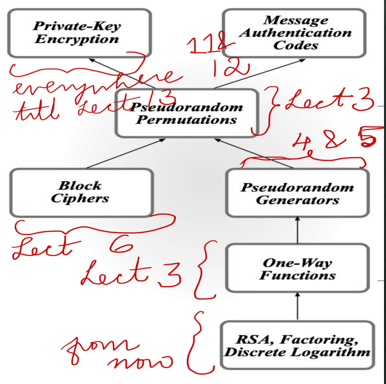
Venturing into Public Key Cryptography

- We have seen that private/secret/symmetric key cryptography (encryption schemes and MACs) can be based on the assumption that pseudorandom permutations/block ciphers exist.
- I.e., there exists some keyed permutation F for which it is hard to distinguish in polynomial time between interactions with F_k (for a uniform, unknown key k) and interactions with a truly random permutation.
- It looks like a strong assumption. But we saw some practical constructions resistant to attacks which gives *an indication that existence of PRPs is plausible*.
- But right now we do not know how to prove the pseudorandomness of any of the practical constructions relative to any *reasonable assumption*.

27/10/2020

Back to OWFs

- It is possible to prove that PRPs exist based on the much milder assumption that one-way functions exist.
- But after Lecture 3 we have not really seen any OWFs.



A top down approach so far.

Number Theory Recap

- The examples of OWFs we see will be number theoretic in nature and so it is important to have a recap of the theory.
- The study of number theory in cryptography will be algorithmic in nature.
- The set of integers are typically denoted as $\mathbb{Z}$.
- We say that a divides b, $a \mid b$ if there exists an integer c s.t. $ac = b$.
- If a does not divide b we write $a \nmid b$.
- We look at cases when all these integers are positive but the definitions typically make sense for negative integers as well.
- Exercise: if $a \mid b$ and $a \mid c$ then $a \mid (xb + yc)$ for any $x, y \in \mathbb{Z}$.
- If $a \mid b$ and a is positive, then we call a a divisor of b and if $a \notin \{1, b\}$ then a is a nontrivial divisor or factor.

Basic Results

- Every integer greater than 1 can be expressed uniquely as product of primes (upto ordering). (Fundamental Theorem of Arithmetic)
- Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Then there exists unique integers q, r for which $a = qb + r$ and $0 \leq r < b$. (Division Algorithm)
- The above q and r can be computed in polynomial time,polynomial in the length of the input.
- What is the length of an integer N? $||N|| = \lfloor log\ N \rfloor + 1$

Basic Results

- The greatest common divisor of $a, b \in \mathbb{Z}$, $gcd(a, b)$ is the largest integer c s.t. $c \mid a$ and $c \mid b$.
- With either a (or b) zero we take gcd as b (or a) and if both are zeroes then gcd is n.d.
- If p is prime $gcd(a, p)$ is either equal to 1 or p.
- If $gcd(a, b) = 1$ then we say a and b are relatively prime.
- Computing gcd in polynomial time : Euclidean Algorithm!
- Let $a, b \in \mathbb{Z}$. Then there exist integers u, v s.t. $ua + vb = gcd(a, b)$. (Extended Euclidean Algorthm)

Euclidean Algorithm

- How to compute the *gcd*, greatest common divisor?
- We are used to factoring but for large numbers that may not be possible. Euclid's algorithm - more efficient.
- Idea – $gcd(r_0, r_1) = gcd(r_0 - r_1, r_1)$.
- We can do this iteratively!

$$gcd(r_0, r_1) = gcd(r_0 \bmod r_1, r_1)$$
$$gcd(r_0, r_1) = gcd(r_1, r_0 \bmod r_1)$$

Euclidean Algorithm

Input Two positive integers, a and b.
Output $g := gcd(a, b)$
Algorithm:$gcd(a, b)$

1. If $a < b$, exchange a and b. Assume w.l.o.g. $a \geq b \geq 0$.
2. If $b = 0$ then output a.
3. Else $gcd(b, a \bmod b)$.

Euclid's Algorithm

$gcd(888, 54) =$

$$888 = 54 * 16 + 24$$
$$54 = 24 * 2 + 6$$
$$24 = 6 * 4 + 0$$

Therefore gcd is 6.

Basic Results

- Let $a, b, N \in \mathbb{Z}$ with $N > 1$.
- $a \bmod N$ denotes the remainder of a upon division by N.
- By division algorithm we have $a \bmod N = r$ where $0 \leq r < N$.
- The mapping of a to $a \bmod N$ is called reduction modulo N.
- If $a \bmod N = b \bmod N$ then we say a and b are congruent modulo N, $a = b \bmod N$.
- Note: $a = b \bmod N$ iff $N \mid (a - b)$.
- The textbook refers to $[a \bmod N]$ as the remainder of a upon division by N.
- E.g: $36 = 21 \bmod 15$ but $36 \neq [21 \bmod 15] = 6$.

Invertible Modulo N

- Congruence modulo N does not in general respect division. I.e., if $a = a' \mod N$ and $b = b' \mod N \not\Rightarrow a/b = a'/b' \mod N$.
- Take $N = 24$, $3 \cdot 2 = 6 = 15 \cdot 2 \mod 24$ but $3 \neq 15 \mod 24$.
- Sometimes it is meaningful to define division or invertible modulo N.
- If for a given integer b there exists an integer c s.t. $bc = 1 \mod N$ then b is invertible modulo N.
- c is a multiplicative inverse of b modulo N.
- 0 is never invertible.
- If c, c' are multiplicative inverses of b modulo N then $c \mod N = c' \mod N$, so we can assume b^{-1} is the unique multiplicative inverse of b that lies in $\{1, \ldots, N-1\}$.

Invertible Modulo N & Groups

- Which integers are invertible modulo a given modulus N?
- Let $b, N \in \mathbb{Z}$ s.t. $b \geq 1$ and $N > 1$. Then b is invertible modulo N iff $gcd(b, N) = 1$.
- Addition, subtraction, multiplication and computation of inverses modulo N can all be carried out in polynomial time.
- We have also seen exponentiation can be carried out in polynomial time.
- What is a Group? A set G with a binary operation $\circ$ for which the following properties hold:
  - Closure: $\forall g, h \in G, g \circ h \in G$.
  - Existence of an identity: There exists an identity $e \in G$ s.t. $\forall g \in G$, $e \circ g = g \circ e = g$.
  - Existence of inverses: $\forall g \in G$, there exists an element $h \in G$ s.t. $g \circ h = e = h \circ g$. h is called an inverse of g.
  - Associativity: $\forall g_1, g_2, g_3 \in G$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

Basics of Groups

- Commutative groups–
- Finite groups with $|G|$ the order of the group.
- Subgroup of G : subset of G that is also a group.
- Usually omit the $\circ$ notation and represent operations as addition or multiplication.
- $\mathbb{Z}$: set of integers is a group w.r.t normal addition but not a group w.r.t. multiplication.
- What about $\mathbb{R}$ the set of real numbers under multiplication? Think about 0!
- The group we will follow in crypto : $\mathbb{Z}_N = \{0, \ldots, N-1\}, + \bmod N$ and $\mathbb{Z}_N^*, \times \bmod N$.
- What is $\mathbb{Z}_N^*$? The set of all invertible elements modulo N.

Important Results from Groups

- Let G be a finite group with $m = |G|$ the order of the group. Then for any element g in G, $g^m = 1$.
- Let G be a finite group with $m = |G|$ the order of the group. Then for any element g in G, and any $x \in \mathbb{Z}$ $g^x = g^{x \bmod m}$.
- Let G be a finite group with $m = |G|$ the order of the group. Let $e > 0$ be an integer and define

$$f_e : G \to G$$
$$f_e(g) = g^e.$$

If $gcd(e, m) = 1$ then f_e is a permutation.

- Also if $d = e^{-1} \bmod m$, then f_d is the inverse of f_e. Since $gcd(e, m) = 1$, e is invertible modulo m.

Group $\mathbb{Z}_N^*$

- In the assignment we saw that taking nonzero elements in $\mathbb{Z}_N$ it can fail to be a group.
- Which elements in $\{1, \ldots, N-1\}$ are invertible? Exactly those for which $gcd(b, N) = 1$.

$$\mathbb{Z}_N^* := \{b \in \{1, \ldots, N-1\} : gcd(b, N) = 1\}.$$

- $\mathbb{Z}_N^*$ is an abelian group under multiplication modulo N. $|\mathbb{Z}_N^*|$ is denoted as $\varphi(N)$, the Euler Totient Function.
- For example $N = 6$,there are two numbers relatively prime to 6 : 1 and 5 and $\varphi(6) = 2$.
- If $N = pq$, where p and q are primes, then $\varphi(N) = (p-1)(q-1)$.

Computing Euler's Phi Function

Theorem

Given the factorization of N,

$$N = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdots {p_n}^{e_n},$$

where the p_is are all distinct primes and e_i are positive integers, then

$$\varphi(N) = \prod_{i=1}^{n} ({p_i}^{e_i} - {p_i}^{e_i - 1}).$$

E.g : $N = 240 = 2^4 \cdot 3 \cdot 5$. We have,
$\varphi(240) = (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0) = 64$.
Computing $\varphi(N)$ is as hard as factoring! If we know the factorization of N then it is easy to calculate $\varphi(N)$.

Euler's Theorem

Theorem

Let a and N be integers with $gcd(a, N) = 1$ *(i.e.* $a \in \mathbb{Z}_N{}^*$*) then:*

$$a^{\varphi(N)} \equiv 1 \; mod \; N.$$

Proof of Euler's Theorem

- Let $A = \{ax : x \in \mathbb{Z}_N{}^*\}$. $A \subseteq \mathbb{Z}_N{}^*$ (since $\mathbb{Z}_N{}^*$ is group)
- If $\mid A \mid < \mid \mathbb{Z}_N{}^* \mid \Rightarrow \exists\, i, j \in \mathbb{Z}_N{}^*$, s.t. $i \neq j$, $ai = aj$ (by pigeonhole principle).
- But a^{-1} exists, multiplying with it on both sides we get $i = j$. Thus $A = \mathbb{Z}_N{}^*$.
- Multiplying elements of $\mathbb{Z}_N{}^*$ and A we get,

$$\prod_{x \in \mathbb{Z}_N{}^*} x \bmod N = \prod_{y \in A} y \bmod N = \prod_{x \in \mathbb{Z}_N{}^*} ax \bmod N$$

$$\prod_{x \in \mathbb{Z}_N{}^*} x \bmod N = a^{\varphi(N)} \prod_{x \in \mathbb{Z}_N{}^*} x \bmod N$$

$$a^{\varphi(N)} \equiv 1 \bmod N.$$

Fermat's Little Theorem - Corollary of Euler's Theorem

In $\mathbb{Z}_p{}^*$, $\varphi(p) = (p^1 - p^0) = p - 1$.

Theorem

Let a be an integer in $\mathbb{Z}_p{}^*$ where p is a prime . Then,

$$a^{p-1} \equiv 1 \ mod \ p.$$

Cyclic Subgroups of G

- We consider a finite group G of order m.
- Take any $g \in G$, the subgroup generated by g is $\langle g \rangle = \{g^0, g^1, \ldots, \}$.
- We know that $g^m = 1$. Can there be a smaller i for which $g^i = 1$? Order of g or its multiples.
- Then $g^i = 0, g^{i+1} = g^1$, and so on..
- So $\langle g \rangle = \{g^0, \ldots, g^{i-1}\}$.
- If i is the smallest integer for which $g^i = 1$ then i is the order of the group generated by g.

Basic Results

- Let G be a finite group and $g \in G$ an element of order i.
  - for any integer x, $g^x = g^{x \bmod i}$
  - Something stronger: $g^x = g^y$ iff $x = y \bmod i$.
- Identity element generates a group of order 1, the only one.
- If there exists g s.t. it has order m then G is a cyclic group and g is a generator, not necessarily the generator!
  - I.e. every element $h \in G$ is of the form g^x for some $x \in \{0, \dots, m-1\}$.
- Let G be a finite group of order m, say $g \in G$ has order i. Then $i \mid m$.
- If G is a group of prime order p, then G is cyclic. All the elements of G are generators except the identity.
- If p is prime then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$. Is every element a generator?

Examples

- Consider $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. It has order $(5-1)(3-1) = 8$.
- $\langle 2 \rangle = \{1, 2, 4, 8\}$. Order of 2 is 4.
- The order 4 divides the order of the group 8. Also 2 is not a generator.
- Should it be necessarily cyclic? In fact $\mathbb{Z}_{15}^*$ is not cyclic.
- Consider $\mathbb{Z}_7^*$. It is cyclic by previous result.
- $\langle 2 \rangle = \{1, 2, 4\}$, so 2 is not a generator.
- 3 is a generator. All elements need not be generators.