Intro. Number Theory

Intractable problems

Easy problems

- Given composite N and x in Z_N find x^{-1} in Z_N

- Given prime p and polynomial $f(x)$ in $Z_p[x]$

  find x in Z_p s.t. $f(x) = 0$ in Z_p (if one exists)

  Running time is linear in deg(f) .

… but many problems are difficult

Intractable problems with primes

Fix a prime p>2 and g in $(Z_p)^*$ of order q.

Consider the function: $\mathbf{x \longmapsto g^x}$ **in $\mathbf{Z_p}$**

Now, consider the inverse function:

$\mathbf{Dlog_g\,(g^x) = x}$ **where x in {0, …, q-2}**

Example:

in $\mathbb{Z}_{11}$:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$\mathrm{Dlog}_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

DLOG: more generally

Let **G** be a finite cyclic group and **g** a generator of G

$$G = \{ 1 , g , g^2 , g^3 , \ \dots \ , g^{q-1} \}$$ (q is called the order of G)

Def: We say that **DLOG is hard in G** if for all efficient alg. A:

$$\Pr_{g \leftarrow G,\ x \leftarrow Z_q} \left[A(G, q, g, g^x) = x \right] < \text{negligible}$$

Example candidates:

(1) $(Z_p)^*$ for large p, (2) Elliptic curve groups mod p

Computing Dlog in $(Z_p)^*$ (n-bit prime p)

Best known algorithm (GNFS): run time exp($\tilde{O}(\sqrt[3]{n})$)

cipher key size	modulus size	Elliptic Curve group size
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	**15360** bits	512 bits

As a result: slow transition away from (mod p) to elliptic curves

An application: collision resistance

Choose a group G where Dlog is hard (e.g. $(Z_p)^*$ for large p)

Let $q = |G|$ be a prime. Choose generators g, h of G

For $x,y \in \{1,\dots,q\}$ define $\boxed{H(x,y) = g^x \cdot h^y}$ in G

Lemma: finding collision for H(.,.) is as hard as computing $Dlog_g(h)$

Proof: Suppose we are given a collision $H(x_0,y_0) = H(x_1,y_1)$

then $g^{x_0} \cdot h^{y_0} = g^{x_1} \cdot h^{y_1} \Rightarrow g^{x_0-x_1} = h^{y_1-y_0} \Rightarrow h = g^{x_0-x_1/y_1-y_0}$ $\neq 0$

Dan Boneh

Intractable problems with composites

Consider the set of integers: (e.g. for n=1024)

$$\mathbb{Z}_{(2)}(n) \;:=\; \{\, N = p \cdot q \quad \text{where } p,q \text{ are n-bit primes} \,\}$$

<u>Problem 1</u>: Factor a random N in $\mathbb{Z}_{(2)}(n)$ (e.g. for n=1024)

<u>Problem 2</u>: Given a polynomial **f(x)** where degree(f) > 1

and a random N in $\mathbb{Z}_{(2)}(n)$

find x in $\mathbb{Z}_N$ s.t. f(x) = 0 in $\mathbb{Z}_N$

The factoring problem

Gauss (1805): *"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."*

Best known alg. (NFS): run time exp($\tilde{O}(\sqrt[3]{n})$) for n-bit integer

Current world record: **RSA-768** (232 digits)

- Work: two years on hundreds of machines
- Factoring a 1024-bit integer: about 1000 times harder

$\Rightarrow$ likely possible this decade

Further reading

- A Computational Introduction to Number Theory and Algebra, V. Shoup, 2008 (V2), Chapter 1-4, 11, 12

Available at **//shoup.net/ntb/ntb-v2.pdf**

End of Segment