6.3 Cryptography

Rabin's One-way Function. Pick random prime numbers $p, q, \|p\| = \|q\|$ with two last bits =1, i.e. with odd $(p-1)(q-1)/4$. Then $n = pq$ is called a Blum number. Its length should make factoring infeasible.

Let $Q_n = (\mathbb{Z}_n^*)^2$ be the set of squares, i.e. ***quadratic residues*** (all residues are assumed $\pmod n$).

Lemma. Let $n = pq$ be a Blum number, $F : x \mapsto x^2 \in Q_n$. Then (1) F is a permutation on Q_n and (2) The ability to invert F on random x is equivalent to that of factoring n.

Proof. (1) $t=(p-1)(q-1)/4$ is odd, so $u=(t+1)/2$ is an integer. Let $x=F(z)$. Both $p-1$ and $q-1$ divide $2t$. So, by Fermat's little theorem, both p, q (and, thus n) divide $x^t-1 \equiv z^{2t}-1$. Then $F(x)^u \equiv x^{2u} = xx^t \equiv x$.

(2) The above y^u inverts F. Conversely, let $F(A(y)) = y$ for a fraction ε of $y \in Q_n$.
Each $y \in Q_n$ has $x, x' \neq \pm x$ with $F(x)=F(x')=y$, both with equal chance to be chosen at random.
If $F(x)$ generates y while $A(y) = x'$ the Square Root Test (5.1) has both x, x' for factoring n. □

Such one-way permutations, called "trap-door", have many applications; we look at cryptography below.

Picking random primes is easy: they have density $1/O(\|p\|)$. Indeed, one can see that $\binom{2n}{n}$ is divisible by every prime $p \in [n, 2n]$ but by no prime $p \in [\frac{2}{3}n, n]$ or prime power $p^i > 2n$. So, $(\log \binom{2n}{n}) / \log n = 2n/\log n - O(1)$ is an upper bound on the number of primes in $[n, 2n]$ and a lower bound on that in $[1, 2n]$ (and in $[3n, 6n]$ as a simple calculation shows). And fast VLSI exist to multiply long numbers and check primality.

Public Key Encryption. A perfect way to encrypt a message m is to add it $\bmod 2$ bit by bit to a random string S of the same length k. The resulting encryption $m \oplus S$ has the same uniform probability distribution, no matter what m is. So it is useless for the adversary who wants to learn something about m, without knowing S. A disadvantage is that the communicating parties must share a secret S as large as all messages to be exchanged, combined. ***Public Key*** Cryptosystems use two keys. One key is needed to encrypt the messages and may be completely disclosed to the public. The ***decryption*** key must still be kept secret, but need not be sent to the encrypting party. The same keys may be used repeatedly for many messages.

Such cryptosystem can be obtained [Blum, Goldwasser 82] by replacing the above random S by pseudo-random $S_i = (s_i \cdot x)$; $s_{i+1} = (s_i^2 \pmod n)$. Here a Blum number $n = pq$ is chosen by the Decryptor and is public, but p, q are kept secret. The Encryptor chooses $x \in \mathbb{Z}_2^{\|n\|}$, $s_0 \in \mathbb{Z}_n$ at random and sends $x, s_k, m \oplus S$. Assuming factoring is intractable for the adversary, S should be indistinguishable from random strings (even with known x, s_k). Then this scheme is as secure as if S were random. The Decryptor knows p, q and can compute u, t (see above) and $v = (u^{k-1} \bmod t)$. So, he can find $s_1 = (s_k^v \bmod n)$, and then S and m.

Another use of the intractability of factoring is digital signatures [Rivest, Shamir, Adleman 78, Rabin 79]. Strings x can be released as authorizations of $y = (x^2 \bmod n)$. Verifying x, is easy but the ability of forging it for generic y is equivalent to that of factoring n.

Go On!

You noticed that most of our burning questions are still open. Take them on!

Start with reading recent results (FOCS/STOC is a good source). See where you can improve them.
Start writing, first notes just for your friends, then the real papers. Here is a little writing advice:

A well written paper has clear components: skeleton, muscles, etc.
The skeleton is an acyclic digraph of basic definitions and statements, with cross-references.
The meat consists of proofs (muscles) each *separately* verifiable by competent graduate students having to read no other parts but statements and definitions cited. Intuitive comments, examples and other comfort items are fat and skin: a lack or excess will not make the paper pretty. Proper scholarly references constitute clothing, no paper should ever appear in public without! Trains of thought which led to the discovery are blood and guts: keep them hidden. Metaphors for other vital parts, like open problems, I skip out of modesty.

Writing Contributions. Section 1 was originally prepared by Elena Temin, Yong Gao and Imre Kifor (BU), others by Berkeley students: 2.3 by Mark Sullivan, 3.1 by Eric Herrmann and Elena Eliashberg, 3.2 by Wayne Fenton and Peter Van Roy, 3.3 by Carl Ludewig, Sean Flynn, and Francois Dumas, 4.1 by Jeff Makaiwi, Brian Jones and Carl Ludewig, 4.2 by David Leech and Peter Van Roy, 4.3 by Johnny and Siu-Ling Chan, 5.2 by Deborah Kordon, 6.1 by Carl Ludewig, 6.2 by Sean Flynn, Francois Dumas, Eric Herrmann, 6.3 by Brian Jones.