Cryptography

Mark Greenstreet, CpSc 421, Term 1, 2008/09

- Today's NP-Completeness Example: Vertex Cover
- Cryptography
  - RSA
  - Cryptography and P vs. NP

Vertex Cover

- Let $G = (V, E)$ be a graph and let $k \in \mathbb{N}$. Does there exist $C \subseteq V$ with $|C| = k$ such that for every edge, $(v_1, v_2) \in E$, $v_1 \in C$, or $v_2 \in C$, or both?
- Vertex cover is NP complete.
  - It is easy to see that vertex cover is in NP – a list of vertices for C suffices as a certificate.
    - Such a list is shorter than the original input, thus its size is polynomial in the length of the input.
    - Checking that the length of the list is k is easy.
    - Checking that each edge of E has at least one vertex in C is straightforward.
  - To show that vertex cover is NP hard, we show that we can reduce 3SAT to vertex cover. We need two "gadgets:"
    - A gadget for each variable of the 3cnf formula to represent the value assigned to the variable.
    - A gadget for each clause of the 3cnf formula to make sure that the clause is satisfied.

Gadgets

Variable Assignment

Clause Satisfaction

Let $k =$

Combining the Pieces

- Every satisfying assignment corresponds to a valid vertex cover.

- Every valid vertex cover corresponds to a satisfying assignment.

The Rumsfeld Hierarchy

As we know,

There are known knowns.

There are things we know we know.

We also know

There are known unknowns.

That is to say

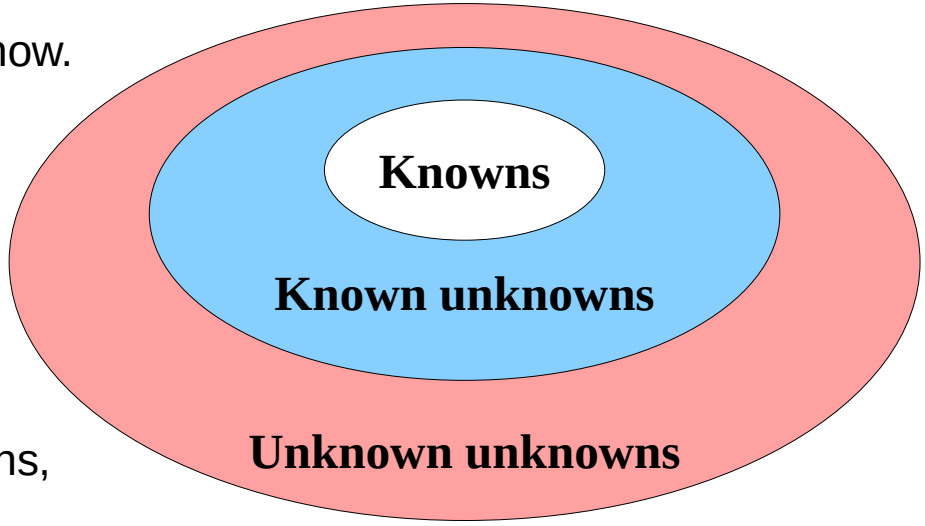
We know there are some things

We do not know.

But there are also unknown unknowns,

The ones we don't know

We don't know.



Donald Rumsfeld, Feb. 12, 2002

From http://www.slate.com/id/2081042/

RSA: key ideas

- Factoring appears to be hard
  - The factoring problem is: given an number, N, find its prime factors (or find any, non-trivial factors).
  - If $P = NP$, then we could factor in polynomial time.
  - No one has shown a way to use an algorithm for factoring to obtain an algorithm for solving a known NP-complete problem.
  - But, many people have tried and failed to find an efficient (i.e. polynomial time) way to factor numbers.
- Finding large prime numbers is easy.
  - This means I can easily find two, large prime numbers, p_1 and p_2.
  - Let $N = p_2 p_2$.
  - I can broadcast N with high confidence that no one will be able to figure out what p_1 and p_2 are.
- RSA turns these observations into an encryption method.

Properties of Primes

- Let p be a prime and n be any number in $\{1 \ldots p-1\}$.
  - $n^{p-1} \bmod p = 1$. (Fermat's little theorem)
  - If $k \bmod (p-1) = 1$, then $n^k \bmod p = n$.
  - In general, these properties don't hold for non-primes.
- There are lots of primes.
  - For large N, about one out of every lnN integers "near" N is prime.
  - To find a large prime,
    - Guess a big number, q.
    - Make sure that it isn't divisible by the first 100 or so primes.
    - Choose some random values for n in $\{1 \ldots p-1\}$.
    - Check that $n^{q-1} \bmod q = 1$.
    - If this passes for a moderate number of trials (and a few other details, see Sipser section 10.2), then we can be quite confident that q is prime.
- This gives us a way to find big primes.

Fermat's Little Theorem (example)

- Let $p = 17$, $n = 5$.
- Calculate $n^{p-1} \bmod p$:

$5^1 \bmod 17$	$=$	$5 \bmod 17$	$=$	5		
$5^2 \bmod 17$	$=$	$(5^1 \bmod 17)^2 \bmod 17$	$=$	$5^2 \bmod 17$		
	$=$	$25 \bmod 17$	$=$	$(17 + 8) \bmod 17$	$=$	8
$5^4 \bmod 17$	$=$	$(5^2 \bmod 17)^2 \bmod 17$	$=$	$8^2 \bmod 17$		
	$=$	$64 \bmod 17$	$=$	$(3 * 17 + 13) \bmod 17$	$=$	13
$5^8 \bmod 17$	$=$	$(5^4 \bmod 17)^2 \bmod 17$	$=$	$13^2 \bmod 17$		
	$=$	$169 \bmod 17$	$=$	$(9 * 17 + 16) \bmod 17$	$=$	16
$5^{16} \bmod 17$	$=$	$(5^8 \bmod 17)^2 \bmod 17$	$=$	$16^2 \bmod 17$		
	$=$	$256 \bmod 17$	$=$	$(15 * 17 + 1) \bmod 17$	$=$	1

A Silly Encryption Scheme

- Choosing a public key:
  - Find a large prime p.
  - Choose a random number $e \in \{2 \ldots p-2\}$ such that e is prime relative to $p-1$.
  - Broadcast p and e.
- To encrypt a message, m.
  - Let $\tilde{m} = m^e \bmod p$.
  - Send $\tilde{m}$.
- To decrypt message:
  - Let $d \in \{2 \ldots p-2\}$ be the number such that $ed \bmod (p-1) = 1$.
  - Compute

$$
\begin{aligned}
\tilde{m}^d \bmod p &= m^{ed} \bmod p, && \tilde{m} = m^e \bmod p \\
&= m^{ed} \bmod p, && \text{algebra} \\
&= m^{k(p-1)+1} \bmod p, && ed \bmod (p-1) = 1 \\
&= (m^{k(p-1)} \bmod p)(m^1 \bmod p) \bmod p, && \text{algebra} \\
&= m, && m^{k(p-1)} = 1 \\
& && \text{(Fermat's little thm.)}
\end{aligned}
$$

A Silly Example

- Choosing a public key.
  - Let $p = 17$, $e = 5$.
- To encrypt a message, m.
  - Let $m = 6$, $\tilde{m} = 6^5 \bmod 17 = 7$.
  - Send 17.
- To decrypt message:
  - Let d be the number such that $ed \bmod (p-1) = 1$; $d = 13$.
  - Compute

$$\begin{aligned} \tilde{m}^d \bmod p &= 7^{13} \bmod 17 \\ &= (7^8)(7^4)(7^1) \bmod 17 \\ &= (16)(4)(7) \bmod 17 \\ &= 448 \bmod 17 \\ &= ((26 * 17) + 6) \bmod 17 \\ &= 6 \end{aligned}$$

- But it's not secure – having broadcast p, anyone can decrypt the message.

RSA Encryption

- Choosing a public key:
  - Find two large primes p_1 and p_2.
  - Let $N = p_1 p_2$, $\phi = (p_1 - 1)(p_2 - 1)$.
  - Choose a random number $e \in \{2 \ldots \phi - 1\}$ such that e is prime relative to ϕ.
  - Broadcast N and e.
- To encrypt a message, m.
  - Let $\tilde{m} = m^e \bmod N$.
  - Send $\tilde{m}$.
- To decrypt message:
  - Let $d \in \{2 \ldots p - 2\}$ be the number such that $ed \bmod (\phi - 1) = 1$.
    - Note that $ed \bmod (p_1 - 1) = ed \bmod (p_2 - 1) = 1$.
    - We can use Euclid's GCD algorithm to find d.
  - Compute $\tilde{m}^d \bmod p = m^{ed} \bmod p = m$.
- Because factoring is (believed to be) intractable,
  - No one else can figure out your private key (d which can be easily computed given p_1 and p_2) from your public key (N and e).

Trapdoor Functions

Digital Signatures

Quantum Computing & Crypto

This coming week (and beyond)

- Reading
  - Nov. 24 (Today): Sipser 10.6
  - Nov. 26 (Wednesday): no reading
  - Nov. 28 (Friday): Sipser 6.1 and 6.2
- Homework
  - Nov. 24 (Today): HW 10 due.
  - Dec. 1 (A week from today): HW 11 due.
- Final Exam:
  - Dec. 6: 3:30-6:30pm
  - CHBE 103