CRYPTOGRAPHY AND COMPLEXITY : PART II of II

6.046

- Symmetric key Encryption
- Key Exchange
- Asymmetric key encryption
- RSA
- NP-complete problems & cryptography
  - graph coloring
  - knapsack.

Symmetric Key Encryption

plaintext

$$c = e_k(m)$$

secret key

Ciphertext

encryption function

$$m = d_k(c)$$

decryption function

e, d permute & reverse-permute

reversible operations $\oplus$ $+/-$, shift left/right

Symmetric algos: AES, RC5, DES

Key Management Question

How does secret key k get exchanged/shared?

Alice

Bob

PIRATES

Boxes
Locks
Keys
message

Boxes
Locks
Keys

Pirates won't touch locked box, but will take away keys, messages in unlocked box(es)

How does Alice send a message to Bob?
(without pirates knowing what was sent)

Solution: Alice puts m in box, locks it with KA
Box sent to Bob
Bob locks box with KB
Box sent to Alice
Alice unlocks KA
Box sent to Bob
Bob unlocks KB, reads m!

Locked Box

Commutative locks! Lock KA, Lock KB, remove KA, remove KB

Diffie-Hellman Key Exchange

$G = F_p^*$ finite field (mod p, a prime)
$*$ means invertible elements only
$\{1, 2, \dots p-1\}$

Alice	g public, p public	Bob
Select a		
Compute g^a	$\longrightarrow$	g^a
		Select b
g^b	$\longleftarrow$	Compute g^b

$2 \le g \le p-2$

$1 \le a, b \le p-2$

Alice can compute $(g^b)^a \bmod p = K$

Bob can compute $(g^a)^b \bmod p = K$

Assumes Discrete Log Problem is hard. Given g^a, compute a

Diffie Hellman Problem is hard. Given g^a, g^b compute g^{ab}

Attack? Man-in-the-middle

Alice doesn't know she is communicating with Bob.

Alice agrees to a key with Eve (thinks she is Bob)

Bob agrees to a key with Eve (thinks she is Alice)

Eve can see all communications

Public Key Encryption

Message + public key = Ciphertext

Ciphertext + private key = Message

Two keys need to be linked in a mathematical way

Knowing the public key should tell you nothing about the private key.

RSA

Alice picks two large secret primes p & q.

Alice computes $N = p \cdot q$

Chooses an encryption exponent e which satisfies

$$\gcd(e, (p-1)(q-1)) = 1 \qquad e = 3, 17, 65537$$

Alice public key $= (N, e)$

Decryption exponent obtained using Extended Euclidean Algorithm by Alice

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

Alice private key $= (d, \underbrace{p, q}_{})$

not absolutely necessary, only for efficiency

ENCRYPTION & DECRYPTION WITH RSA

$$c = m^e \pmod N \quad \text{encryption}$$
$$m = c^d \pmod N \quad \text{decryption}$$

Why it works

$$\phi = (p-1)(q-1)$$

Since $ed \equiv 1 \pmod \phi$ there exists an integer k such that $ed = 1 + k\phi$

Two cases:

1) $\gcd(m, p) = 1$ By Fermat's theorem

$$m^{p-1} \equiv 1 \pmod p$$
$$\left(m^{p-1}\right)^{k(q-1)} \cdot m \equiv m \pmod p$$
$$m^{1+k(p-1)(q-1)} = m^{ed} \equiv m \pmod p$$

2) $\gcd(m, p) = p$ $\quad m \bmod p = 0$

trivial case $m^{ed} \equiv m$

$\therefore$ in both cases $m^{ed} \equiv m \pmod p$

$\|^{ly}$ $\quad m^{ed} \equiv m \pmod q$

Since p & q are distinct primes

$$m^{ed} \equiv m \pmod N$$

So $c^d = (m^e)^d \equiv m \pmod N$

HARDNESS OF RSA

1) Given N, hard to factor into p, q — Factoring

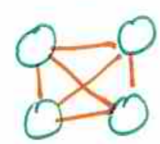
2) Given e such that
$$\gcd(e, (p-1)(q-1)) = 1$$
and c, find m such that
$$m^e = c \pmod N$$
— RSA Problem

NP- Completeness

Is N composite? $\in NP$ — unknown if NP-complete
with a factor within a range

Is a graph k-colorable? — NP-complete
Assign k colors to each vertex such that no two vertices connected by an edge share the same color

not 3-colorable



Given a pile of n items, each with different weights w_i, is it possible to put items in a knapsack such that we get a specific weight S? — NP-complete
$$S = b_1 w_1 + b_2 w_2 + \dots b_n w_n \, ?$$

NP-completeness & Cryptography

NP-completeness: about worst-case complexity
Cryptography: want a problem instance, with suitably chosen parameters that is hard on average.

Most Knapsack cryptosystems have failed.

Determining if a graph is 3-colorable is NP-complete
But very easy on average, because average graph, beyond a certain size, is not 3-colorable!

Consider standard backtracking search to determine 3-colorability.

Order vertices $v_1, \ldots v_t$. Colors $= \{1, 2, 3\}$
Traverse graph in order of vertices
On visiting a vertex, choose smallest possible color that "works".
If you get stuck, backtrack to previous choice, and try next choice
Run out of colors for 1st vertex $\longrightarrow$ NOT
Successfully color last vertex $\longrightarrow$ YES.

Random graph of t vertices, average number of vertices traveled < 197, REGARDLESS of t!

KNAPSACK CRYPTOGRAPHY

General knapsack problem: NP-complete

Super-increasing knapsacks: linear time solvable

$$w_j \geq \sum_{i=1}^{j-1} w_i \qquad \{2, 3, 6, 13, 27, 52\}$$

Merkle Hellman Cryptosystem:

Private key $\rightarrow$ super increasing knapsack problem

$\downarrow$ PRIVATE TRANSFORM

Public key $\leftarrow$ "hard" general knapsack problem

Transform: two private integers N, M s.t. $\gcd(N, M) = 1$

Multiply all values in the sequence by N, and then mod M.

$N = 31$, $M = 105$ private key = $\{2, 3, 6, 13, 27, 52\}$

public key = $\{62, 93, 81, 88, 102, 37\}$.

MERKLE-HELLMAN EXAMPLE

Message = 011000 110101 101110

Ciphertext : 011000 $93 + 81 = 174$

110101 $62 + 93 + 88 + 37 = 280$

101110 $62 + 81 + 88 + 102 = 333$

$= 174, 280, 333$

Recipient knows $N = 31$, $M = 105$ $\{2, 3, 6, 13, 27, 52\}$

Multiplies each ciphertext block by $N^{-1} \pmod{M}$

$N^{-1} = 61 \pmod{105}$

$174 \cdot 61 = 9 = 3 + 6 = 011000$

$280 \cdot 61 = 70 = 2 + 3 + 13 + 52 = 110101$

$333 \cdot 61 = 48 = 2 + 6 + 13 + 27 = 101110$

BEAUTIFUL BUT BROKEN

Lattice based techniques break this scheme.

Density of knapsack $d = \dfrac{n}{\max\{\log_2 w_i : 1 \le i \le n\}}$

Lattice basis reduction can solve knapsacks of low density. Unfortunately M-H scheme always produces knapsacks of low density!

[on average, easy to solve!