Introduction to Modern Cryptography

Lecture 7

1. RSA Public Key CryptoSystem
2. One way Trapdoor Functions

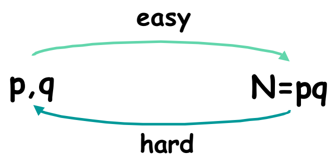
Diffie and Hellman (76) “New Directions in Cryptography”

Split the Bob’s secret key K to two parts:

- K_E , to be used for encrypting messages to Bob.
- K_D , to be used for decrypting messages by Bob.

K_E can be made public
(public key cryptography,
assymetric cryptography)

Integer Multiplication & Factoring as a One Way Function.



Q.: *Can a public key system be based on this observation ?????*

Excerpts from RSA paper (CACM, Feb. 78)

The era of “electronic mail” may soon be upon us; we must ensure that two important properties of the current “paper mail” system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a “public-key cryptosystem,” an elegant concept invented by Diffie and Hellman. Their article motivated our research, since they presented the concept but not any practical implementation of such system.

The Multiplicative Group Z_{pq}*

Let p and q be two large primes.
Denote their product N = pq .
The multiplicative group $Z_N^* = Z_{pq}^*$ contains all integers in the range [1,pq-1] that are relatively prime to both p and q.

The size of the group is
$\phi(pq) = (p-1)(q-1) = N - (p+q) + 1$,
so for every $x \in Z_{pq}^*$, $x^{(p-1)(q-1)} = 1$.

Exponentiation in Z_{pq}*

Motivation: We want to exponentiation for encryption.

Let e be an integer, $1 < e < (p-1)(q-1)$.

Question: When is exponentiation to the e^{th} power, $x \to x^e$, a one-to-one op in Z_{pq}^* ?

Exponentiation in Z_{pq}^*

Claim: If e is relatively prime to (p-1)(q-1) then $x \dashrightarrow x^e$ is a one-to-one op in Z_{pq}^*

Constructive proof: Since gcd(e, (p-1)(q-1))=1, e has a multiplicative inverse mod (p-1)(q-1). Denote it by d, then ed = 1 + C(p-1)(q-1).

Let $y=x^e$, then $y^d=(x^e)^d=x^{1+C(p-1)(q-1)}=x$ mod pq meaning $y \dashrightarrow y^d$ is the inverse of $x \dashrightarrow x^e$ QED

RSA Public Key Cryptosystem

- Let N=pq be the product of two primes
- Choose e such that gcd(e,ϕ(N))=1
- Let d be such that ed$\equiv$1 mod ϕ(N)
- The public key is (N,e)
- The private key is d
- Encryption of $M \in Z_N^*$ by $C=E(M)=M^e$ mod N
- Decryption of $C \in Z_N^*$ by $M=D(C)=C^d$ mod N

"The above mentioned method should not be confused with the exponentiation technique presented by Diffie and Hellman to solve the key distribution problem".

Constructing an instance of RSA PKC

- Alice first picks at random two large primes, p and q.
- Alice then picks at random a large d that is relatively prime to (p-1)(q-1) (gcd(d,ϕ(N))=1).
- Alice computes e such that de$\equiv$1 mod ϕ(N)

- Let N=pq be the product of p and q.
- Alice publishes the public key (N,e).
- Alice keeps the private key d, as well as the primes p, q and the number ϕ(N), in a safe place.
- To send M to Alice, Bob computes M^e mod N.

A Small Example

Let p=47, q=59, N=pq=2773. ϕ(N)= 46*58=2668.

Pick d=157, then 157*17 - 2668 =1, so e=17 is the inverse of 157 mod 2668.

For N =2773 we can encode two letters per block, using a two digit number per letter: blank=00, A=01,B=02,...,Z=26.

Message: ITS ALL GREEK TO ME is encoded

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

A Small Example

N=2773, e=17 (10001 in binary).

ITS ALL GREEK TO ME is encoded as

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

First block M=0920 encrypts to

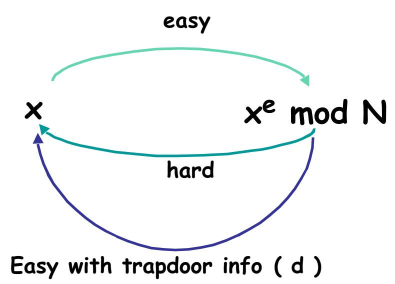
$M^e= M^{17} = (((M^2)^2)^2)^2 * M = 948$ (mod 2773)

The whole message (10 blocks) is encrypted as

0948 2342 1084 1444 2663 2390 0778 0774 0219 1655

Indeed $0948^d=0948^{157}=920$ (mod 2773), etc.

RSA as a One Way Trapdoor Function.



Trap-Door OWF

- Definition: $f: D \to R$ is a *trap-door one way function* if there is a trap-door s such that:
  - Without knowledge of s, the function f is a one way function
  - Given s, inverting f is easy
- Example: $f_{g,p}(x) = g^x \bmod p$ is not a trap-door one way function.
- Example: RSA is a trap-door OWF.

Attacks on RSA

1. Factor N=pq. This is believed hard unless p,q have some "bad" properties. To avoid such primes, it is recommended to

- Take p, q large enough (100 digits each).
- Make sure p, q are not too close together.
- Make sure both (p-1), (q-1) have large

prime factors (to foil Pollard's rho algorithm).

Attacks on RSA

- Find $\phi(N) = (p-1)(q-1)$.

This enables factoring N as from pq = N, $pq-p-q+1 = \phi(N)$ we compute $p+q=N-\phi(N)+1$. Then we solve (over Q) pq = A and p+q = B.

- Find the secret key d.

This also enables the efficient factoring of N, by a more sophisticated argument (due to Miller).

Factoring N Given d: Goal

We'll show that given d,e,N (N=pq), one can factor N efficiently(random poly-time in log N).

Therefore, any efficient procedure of producing d, given just e and N, yields an efficient procedure for factoring N.

Conclusion:
Infeasibility to factor N given e implies infeasibility to find d given N and e.

Factoring N Given d

Input: d,e,N.

Both d and e must be odd since they are relatively prime to (p-1)(q-1). By construction $ed = 1 \bmod \phi(N)$. Let $ed - 1=2^k r$ (r is odd).

Pick b at random (1<b<N).

If gcd(b,N)>1, we are done.

Else $b \in Z_N^*$, so $b^{ed-1} = 1 \bmod N$.

Factoring N Given d (cont.)

Input: d,e,N.

Let $ed-1=2^k r$ where r is odd, $b^{ed-1} = 1 \bmod N$.

Compute mod N

$a_0 = b^r$, $a_1 = (a_0)^2$, $a_2 = (a_1)^2$,…, $a_k = (a_{k-1})^2$.

1. We know $a_k = 1$. Let j be the smallest index with $a_j = 1 \bmod N$.
2. If 0 < j and $a_{j-1} \neq N-1$ then a_{j-1} is a non trivial square root of 1 mod N.

Factoring N Given d (cont.)

Theorem: At least half the b, 1<b<N, yield a non trivial square root of 1 mod N.

Proof omitted.

Claim: If $x^2 = 1$ mod N and $x \neq 1$, N-1 then gcd(x+1,N)>0 .

Proof: $x^2 - 1 = (x+1)(x-1)$. N divides the product, but $x \neq$ N- 1, 1. Thus N does not divide (x-1) or (x+1), so p must divide one of them and q must divide the other term QED

Factoring N Given d: Algorithm

Input: d,e,N. Pick b at random

Let $ed-1=2^k r$ where r is odd, $b^{ed-1} = 1$ mod N.

Compute mod N

$a_0 = b^r$, $a_1 = (a_0)^2$, $a_2 = (a_1)^2, \ldots, a_k = (a_{k-1})^2$.

By theorem, with prob > 0.5 one of the a_j is a non trivial square root of 1 mod N. Such root yields N's factorization.

All ops are poly-time in log N QED

Factoring N Given d: Small Example

Input: N =2773 ,e=17,d =157.

$ed-1=2668=2^2*667$.

Pick b at random. Operations mod 2773.

1. b=7. $7^{667}= 1$. No good…
2. b=8. $8^{667}= 471$, and $471^2= 1$, so 471 is a non trivial square root of 1 mod 2773.

Indeed

gcd (472,N)=59, gcd (470,N)=47.

QED

Real World usage of RSA

1. Key Exchange
2. Digital Signatures (future lecture)