IoT Security and Privacy

Introduction to RSA

YIER JIN

UNIVERSITY OF FLORIDA

EMAIL: YIER.JIN@ECE.UFL.EDU

SLIDES ARE ADAPTED FROM ONLINE RESOURCES

The Public Key Concept

The RSA Algorithm

Knapsack problems

Discrete Logarithms by ElGamal

Error Correcting Codes by McEliece

Elliptic Curve Cryptosystem by Diffie-Hellman

The Concept and Criteria

$E_k(D_k(m))=m$ and $D_k(E_k(m))=m$ for every message m in M, the set of possible messages, every key k in K, the set of possible keys

For every m and every k, then values of $E_k(m)$ and $D_k(m)$ are easy to compute

For every k, if someone knows only the function E_k, it is computationally infeasible to find an algorithm to compute D_k

Given k, it is easy to find the functions E_k and D_k

RSA (Rivest, Shamir, Adleman)

Based on the idea that factorization of integers into their prime factors is hard.

★ $n = p \times q$, where p and q are distinct primes

Proposed by Rivest, Shamir, and Adleman in 1977 and a paper was published in The Communications of ACM in 1978

A public-key cryptosystem

Hard Problems

Some problems are hard to solve.

- No polynomial time algorithm is known.
- e.g., NP-hard problems such as machine scheduling, bin packing, 0/1 knapsack, finding prime factors of an n-digit number.

Is this necessarily bad?

No! Data encryption relies on difficult to solve problems.

Public Key Cryptosystem (RSA)

A public encryption method that relies on a public encryption algorithm, a public decryption algorithm, and a public encryption key.

Using the public key and encryption algorithm, everyone can encrypt a message.

The decryption key is known only to authorized parties.

RSA Algorithm

Bob chooses two primes p,q and compute n=pq

Bob chooses e with

gcd(e,(p-1)(q-1))=

gcd(e, ψ(n))=1

Bob solves de≡1 (mod ψ(n))

Bob makes (e,n) public and (p,q,d) secret

Alice encrypts M as $C \equiv M^e \pmod{n}$

Bob decrypts by computing $M \equiv C^d \pmod{n}$

Proof for the RSA Algorithm

$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M \pmod{n}$ by Euler's theorem

p=885320963, q=238855417,

n=p×q=211463707796206571

Let e=_____, ∴ d=______________________

M="cat"=30120, C=___________________________

Proof for the RSA Algorithm

$C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\phi(n)} \equiv M \pmod{n}$ by Euler's theorem

p=885320963, q=238855417,

n=p×q=211463707796206571

Let e=9007, ∴ d=116402471153538991

M="cat"=30120, C=113535859035722866

Another Example

$n=127 \times 193=24511$, $\phi(n)=24192$

$e=1307$, $d=10643$

Encrypt "box" with M=21524, then

C=?

Encrypt the following message

Formosa means a beautiful island

More RSA Examples

n=11413=101x113, so p=101, q=113

ψ(n)=(p-1)x(q-1)=100x112=11200

Choose e=7467, then gcd(e, ψ(n))=1

Solve de≡1 (mod ψ(n)) to get d=3

If the ciphertext C=5859, then the plaintext

$M \equiv C^d \equiv 5859^3 \equiv 1415 \pmod{11413}$

Fast Computation of $x^d \pmod{n}$

$123^5 \bmod 511$

$123^5 \equiv 28153056843 \bmod 511$

$123^2 \equiv 310 \pmod{511}$

$123^4 \equiv 32 \pmod{511}$

$123^5 \equiv 123^{101b} \equiv 123^4 \times 123$

$\equiv 359 \pmod{511}$

Two Claims

Claim 1: Suppose n=pq is the product of two distinct primes. If we know n and $\phi(n)$, then we can quickly find p and q

Hint: $n - \phi(n)+1=pq-(p-1)(q-1)+1=p+q$, then

p,q are solutions of $x^2 - (n - \phi(n)+1)x+n=0$

Claim 2: If we know d and e, then we can probably factor n (The method of universal components could be applied)

Primality Testing

Trivial Division to test if N is a prime

```
for (p=2; p<N^(1/2); p++) {
    e=0;
    if (N%p ==0 ) {
      while (N%p ==0) { e++; N/=p;}
      printf("factor %d,  power %d\n",p,e);
    }
  }
```

$p < N^{1/2}$

The Miller-Rabin Primality Test

Let $n>1$ be odd with $n-1=2^k m$ with an odd m.

Choose a random integer a, $1<a<n-1$.

Compute $b_0 \equiv a^m \pmod{n}$, if $b_0 \equiv \pm 1 \pmod{n}$, then stop and n is probably prime, otherwise let $b_1 \equiv (b_0)^2 \pmod{n}$.

If $b_1 \equiv 1 \pmod{n}$, then n is composite and $\gcd(b_0-1,n)$ is a nontrivial factor of n else if $b_1 \equiv -1 \pmod{n}$, stop and n is probably prime, otherwise let $b_2 \equiv (b_1)^2 \pmod{n}$.

If $b_2 \equiv 1 \pmod{n}$, then n is composite, else if $b_2 \equiv -1 \pmod{n}$, stop and n is probably prime. Continue in this way until stopping or reaching b_{k-1}.

If $b_{k-1} \,!\!\equiv -1$, then n is composite.