EECS 3481 APPLIED CRYPTOGRAPHY

ASYMMETRIC CRYPTO
aka PUBLIC-KEY Crypto

PROF H ROUMANI
Dept. of Electrical Engineering and Computer Science, York University

1

THE IDEA

Alice and Bob never need to meet!

- Bob chooses two keys: a public and a private one.
- Everyone knows the public key (*critical*).
- Only Bob knows the private key (*critical*).
- Alice encrypts with Bob's public key and sends.
- Upon receipt, Bob decrypts with his private key.
- Most popular: RSA

2

2

USE CASE

- I know Amazon's public key
- I use it to encrypt my credit card and send the ciphertext
- Only Amazon can decrypt

Inefficient but you get confidentiality w/o a prior meeting. Vital for eCommerce.

3

3

USE CASE, CONTINUED

Q

But how does Amazon encrypt the response (I don't have a public/private pair)?

A

Augment with symmetric crypto: generate a random secret key (e.g. AES) for session and send it to Amazon encrypted with its public key. Afterwards, the entire session is secure.

By-Product: Efficiency!

4

4

ALGORITHMS

1. RSA (Factorization)
2. Diffie Hellman (Discrete Log)
3. El-Gamal (Discrete Log)
4. ECC (Elliptic Curve)
5. NTRUE, Paillier, Cramer-Shoup

Classification: Information-Theoretic, Computationally, Provably, or Practically Secure Algorithms

5

5

RSA

RIVEST–SHAMIR–ADLEMAN

6

RSA is Computationally Secure

Deriving the private from the public amounts to factoring

What are the factors of: [100 digits]

1522605027922533360535618378132637429718068114961380688657908494580122963258952897654000350692006139

They are: [50 digits]

37975227936943673922808872755445627854565536638199

and: [50 digits]

40094690950920881030683735292761468389214899724061

See http://en.wikipedia.org/wiki/RSA_numbers#RSA-100

7

7

RSA – What

- Terminology
  modulus: n (public),
  public exponent: e,
  private exponent: d
- The Plaintext
  Express as a (big) integer m < n
  (use mode of op if m >= n)
- Algorithm
  Encryption function E: $c = m^e \bmod n$
  Decryption function D: $m = c^d \bmod n$

8

8

RSA Example

e = 7, d = 103, n = 143

m ∈ {PT}, c ∈ {CT},

c = E(m) = m^7 % 143

m = D(c) = c^{103} % 143

For example,

if m = 2 → c = E(2) = 128

if c = 128 → m = D(128) = 2

9

9

RSA – How

1. Pick two large primes p and q. n = pq
2. Compute phi = (p-1)(q-1)
3. Pick phi > e > 1 such that GCD(e, phi) = 1
4. Compute d = inverse of e mod phi
5. Destroy p, q, and phi
6. Make n,e public; keep d private

10

10

Example

```
p = 11, q = 13
n = 143, phi = 120
e = 7
d = 103

Public Key:  (143, 7)
Private Key: (143, 103)

Encrypt/Decrypt m = 30
Sign/Verify m = 30
```

11

11

Mathematical Prelude

- What is a prime number?
- How many primes less than x? ≅ x/lnx
- How to Add, Subtract, and Multiply mod n?
- How to Divide mod n?
- Exponentiate mod n: direct, recursive, squaring
- Exponentiate Faster: Fermat and Euler

12

12

Fermat & Euler Examples

Fermat: $GCD(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Q: $m = 15$, compute $m^{155} \pmod{23}$
A: since $GCD(15,23)=1$ and $155=22*7+1$,
$m^{155} \equiv (m^{22})^7 * m \equiv 15$

Euler: $GCD(a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Q: $m = 5$, compute $m^{155} \pmod{12}$
A: since $GCD(5,12)=1$ and $\varphi(12)=4$,
$m^{155} \equiv m^{152} * m^3 \equiv m^{38*4} * m^3 \equiv 5$

Note $\varphi(n)$ is easy to compute if n is prime or a product of two primes

13

13

RSA – Why

- Prove the algorithm if m does not divide n:

$c \equiv m^e$ and $GCD(m,n) = 1$
$\Rightarrow$
$c^d \equiv m$

- Extend the proof if m | n
  Note that this case is very unlikely, why?
  Nevertheless: m|n implies m is a multiple of p or q *but not both.*
  So …

14

14

Selected RSA Attacks

- Leaked Key Spec
  For example, if we know q, we can compute p, phi, hence d.
- Very Low m and e
  Take the e'th root if mod hasn't kicked in → must pad
- Chosen Ciphertext
  Given c, we can find m as follows: choose $c' = c * 2^e$ and ask the engine to decrypt. This yields 2m and thus m.
- Short Plaintext
  Given a short m such as a 56b DES key, finding it given c and e requires 10^{17} trials. But if we assume m=xy then we can sit in the middle in between cx^{-e} and y^e (x,y in 1…10^9)

15

15

Primality (Compositeness) Testing I

- The Fermat Test

  Simply compute a^{r-1} (mod r). If not 1 then r is not prime, else the test fails (and we say r is pseudoprime for base a).r=35 is pseudoprime with base 29, but not with base 2. Carmichael numbers (561, 1105, …) are pseuodoprimes with every base. When Fermat succeeds, it doesn't tell us how yo factor.

- The "Square-Root" Test

  If $x^2 \equiv_r y^2$ and $x \mathrel{!\equiv_r} \pm y$ then r is composite; factor=GCD(x-y, r). If this factor is 1 then x=-y and if it is r then x=y and both are contrary to assumption. Hence, it is a non-trivial factor of r. This shows compositeness and provide the factors. $12^2 =_{35} 2^2$ proves that 35 is composite with factor GCD(10,35)=5.

16

16

Primality Testing II

- Miller-Rabin Test

  Start with Fermat. If it fails, recast it as a square root test with e=(r-1)/2 since r is odd. If a^e is not ∓ 1 then composite; if = 1 then repeat; and if = -1 then inconclusive. Try Carmichael 561 with base 2, and you can show it composite and find factors. $2^{560}=1$, $2^{280}=1$, $2^{140}=67$ => GCD(2^{140} -1,561)=GCD(66,561)=11. If inconclusive, it is a strong pseudoprime for that base.

- Monte Carlo Prime Generation

  Start with a random with the desired size and increment by 2. Test each by generating **s** random bases and do M-R on each. Probability of a false positive is ¼ per base. Certainty = $1-(¼)^s$.

17

17