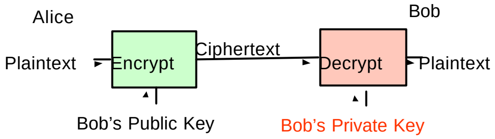
Lecture 8: Non-secret Key Cryptosystems (How Euclid, Fermat and Euler Created E-Commerce)

Real mathematics has no effects on war. No one has yet discovered any warlike purpose to be served by the theory of numbers.
G. H. Hardy, *The Mathematician's Apology,* 1940.

CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Public-Key Applications: Privacy



Alice

Bob

Plaintext

Encrypt

Ciphertext

Decrypt

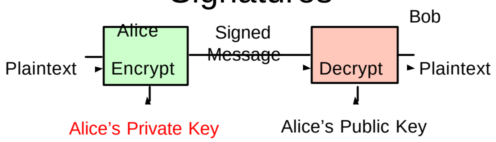
Plaintext

Bob's Public Key

Bob's Private Key

- Alice encrypts message to Bob using Bob's Private Key
- Only Bob knows Bob's Private Key ⇒ only Bob can decrypt message

Signatures



Bob

Alice

Plaintext

Encrypt

Signed Message

Decrypt

Plaintext

Alice's Private Key

Alice's Public Key

- Bob knows it was from Alice, since only Alice knows Alice's Private Key
- Non-repudiation: Alice can't deny signing message (except by claiming her key was stolen!)
- Integrity: Bob can't change message (doesn't know Alice's Private Key)

Public-Key Cryptography

- Private procedure: E
- Public procedure: D
- Identity: $\mathrm{E}(\mathrm{D}(m)) = \mathrm{D}(\mathrm{E}(m)) = m$
- Secure: cannot determine E from D
- But didn't know how to find suitable E and D

Properties of E and D

Trap-door one way function:

1. $D(E(M)) = M$
2. E and D are easy to compute.
3. Revealing E doesn't reveal an easy way to compute D

Trap-door one way permutation: also

4. $E(D(M)) = M$

RSA

$E(M) = M^e \bmod n$

$D(C) = C^d \bmod n$ (red = secret)

$n = pq$ p, q are prime

d is relatively prime to $(p-1)(q-1)$

$ed \equiv 1 \pmod{(p-1)(q-1)}$

RSA in Perl

```
print pack"C*", split/\D+/,
```

Until 1997 – Illegal to show this slide to non-US citizens!

```
/dsM0<J]dsJxp"|dc`
```

(by Adam Back)

Until Jan 2000: can export RSA, but only with 512 bit keys
Now: can export RSA except to embargoed destinations

First Amendment

Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment.

Sixth Circuit Court of Appeals, April 4, 2000
Ruling that Peter Junger could post RSA source code on his web site

Properties of E and D

Trap-door one way function:

1. $D(E(M)) = M$
2. E and D are easy to compute.
3. Revealing E doesn't reveal an easy way to compute D

Trap-door one way permutation: also

4. $E(D(M)) = M$

Property 1: $D(E(M)) = M$

$E(M) = M^e \bmod n$

$D(E(M)) = (M^e \bmod n)^d \bmod n$

$= M^{ed} \bmod n$ (as in D-H proof)

Can we choose e, d and n so:

$M \equiv M^{ed} \bmod n$

$1 \equiv M^{ed-1} \bmod n$

Euler's totient (phi) function

- $j(n)$ = number of positive integers < n which are relatively prime to n.
- If n is prime, $j(n) = n - 1$.
  - Proof by contradiction.

Totient Products

For primes, p and q: $n = pq$

$j(n) = j(pq)$

$j(n)$ = numbers < n **not** relatively prime to pq

$= pq - 1$ numbers less than pq

$- p, 2p, 3p, \ldots, (q-1)p$; q-1 of them

$- q, 2q, 3q, \ldots, (p-1)q$; p-1 of them

$= pq - 1 - (q-1) - (p-1)$

$= pq - (p + q) + 1$

$= (p-1)(q-1) = j(p)\, j(q)$

Euler's Theorem

- For a and n relatively prime:

$$a^{j\,(n)} \equiv 1 \bmod n$$

- Recall: we are looking for e, d and n such that:

$$M^{ed\text{-}1} \equiv 1 \bmod n$$

Fermat's Little Theorem

If n is prime and a is not divisible by n

$$a^{n\text{-}1} \equiv 1 \bmod n$$

Stronger version: (in MBC p. 200):

If n is prime, for any a:

$$a^{n} \equiv a \bmod n$$

Fermat's Little Theorem Proof

$\{a \bmod n, 2a \bmod n, \ldots , (n\text{-}1)a \bmod n\} = \{1, 2, \ldots, (\mathrm{n} - 1) \}$

if $ab \bmod n = ac \bmod n$

and a is relatively prime to n

then $b = c \bmod n$

Fermat's Little Theorem Proof

$\{a \bmod n, 2a \bmod n, \ldots , (n\text{-}1)a \bmod n\} = \{1, 2, \ldots, (n - 1) \}$

$$a \times 2a \times \ldots \times (n - 1)\, a \equiv (n - 1)! \bmod n$$

$$(n - 1)!a^{n\text{-}1} \equiv (n - 1)! \bmod n$$

$$a^{n\text{-}1} \equiv 1 \bmod n$$

Euler's Theorem

For a and n relatively prime:

$$a^{j\,(n)} \equiv 1 \bmod n$$

Proof:

If n is prime, $j\ (n) = n - 1$ and

$$a^{n\text{ - }1} \equiv 1 \bmod n$$

by Fermat's Little Theorem.

What if n is not prime?

Euler's Theorem, cont.

For a and n relatively prime:

$$a^{j\,(n)} \equiv 1 \bmod n$$

$j\ (n)$ = number of numbers $< n$ **not** relatively prime to n

We can write those numbers as:

$$\mathrm{R} = \{ x_1, x_2, \ldots , x_{j(n)}\}$$

Proving Euler's Theorem

$R = \{ x_1, x_2, \dots , x_{j(n)}\}$ multiply by $a \bmod n$:

$S = \{ ax_1 \bmod n, ax_2 \bmod n, \dots, ax_{j(n)} \bmod n\}$

S is a permutation of R:

– a is relatively prime to n and x_i so ax_i is relatively prime to n hence all elements of S are in R.

– There are no duplicates in S.

If $ax_i \bmod n = ax_j \bmod n$ then $i = j$. since a is relatively prime to n.

Proving Euler's Theorem

$$x_1 \times x_2 \dots \times x_{j(n)}$$

$$= ax_1 \bmod n \times ax_2 \bmod n \dots \times ax_{j(n)} \bmod n$$

$$\equiv (ax_1 \times ax_2 \dots \times ax_{j(n)}) \bmod n$$

$$\equiv a^{j(n)} \times x_1 \times x_2 \dots \times x_{j(n)} \bmod n$$

$$1 \equiv a^{j(n)} \bmod n \qquad \text{QED.}$$

Recap

- Euler's Theorem: $1 \equiv a^{j(n)} \bmod n$

  $\boxed{\text{for } a \text{ and } n \text{ relatively prime}}$ What if M is not relatively prime to n?

- If n is prime, $j(n) = n - 1$.
- For p and q prime, $j(pq) = j(p)j(q)$
- We are looking for e, d and n such that:

$$M^{ed-1} \equiv 1 \bmod n$$

$$ed - 1 = j(n) = (p-1)(q-1)$$

M and n

- Suppose M and n not relatively prime:

  $\gcd(M, n) \neq 1$

- Since $n = pq$ and p and q are prime:

  $\gcd(M, p) \neq 1$ OR $\gcd(M, q) \neq 1$

Case 1: $M = cp$

$\gcd(M, q) = 1$ (otherwise M is multiple of both p and q, but $M < pq$).

So, $M^{j(q)} \equiv 1 \bmod q$

(by Euler's theorem, since M and q are relatively prime)

M and n, cont

Case 1: $M = cp$

$\gcd(M, q) = 1$ (otherwise M is multiple of both p and q, but $M < pq$).

So, $M^{j(q)} \equiv 1 \bmod q$

(by Euler's theorem, since M and q are relatively prime)

$$M^{j(q)} \equiv 1 \bmod q$$

$$(M^{j(q)})^{j(p)} \equiv 1 \bmod q$$

$$M^{j(q)j(p)} \equiv 1 \bmod q$$

$$M^{j(n)} \equiv 1 \bmod q$$

M and n

$M^{j(n)} \equiv 1 \bmod q$

$M^{j(n)} = 1 + kq$ for some k

$M = cp$ recall $\gcd(M, p) \neq 1$

$M \times M^{j(n)} = (1 + kq)cp$

$M^{j(n)+1} = cp + kqcp = M + kcn$

$M^{j(n)+1} \equiv M \bmod n$

Where's ED?

$$ed - 1 = j\ (n) = (p\text{-}1)(q\text{-}1)$$

- So, we need to choose e and d:

  $ed = j\ (n) + 1 = n - (p + q)$
- Pick random d, relatively prime to $j\ (n)$

  $\gcd(d, j\ (n)) = 1$
- Since d is relatively prime to $j\ (n)$ it has a multiplicative inverse e:

  $de \equiv 1 \bmod j\ (n)$

Identity

$$de \equiv 1 \quad \bmod j\ (n)$$

So, $d * e = (k * j\ (n)) + 1$ for some k.

Hence,

$$M^{ed\text{-}1} \bmod n = M^{k * j\ (n)} \bmod n$$

$D\,(E\,(M)) = M$

$$M^{ed\text{-}1} \bmod n = M^{k * j\ (n)} \bmod n$$

Euler says $1 \equiv M^{j\ (n)} \bmod n.$

So $1 \equiv M^{k * j\ (n)} \bmod n$

$1 \equiv M^{ed\text{-}1} \bmod n$

$M \equiv M^{ed} \bmod n$

QED.

Properties of E and D

Trap-door one way function:

✓ 1. $D\,(E\,(M)) = M$

➡ 2. E and D are easy to compute.

3. Revealing E doesn't reveal an easy way to compute D

Trap-door one way permutation: also

4. $E\,(D\,(M)) = M$

Property 2: Easy to Compute

- $E(M) = M^e \bmod n$
- Easy – every 4th grader can to exponents, every kindergartner can do mod n.
- How big are M, e, and n?
  - M: 2^n where n is the number of bits in M
  - M and n must be big (~10^{200}) for security

Fast Exponentiation

- $a^{m+n} = a^m * a^n$
- $a^b = a^{b/2} * a^{b/2}$ (if 2 divides b)
- So, can compute M^e in about $\log_2 e$ multiplies
- $10^{150} < 2^{512}$, 512 multiplies is doable (by a computer, not a kindergartner)
- Faster bitwise algorithms known

Anything else hard to compute?

- We need to find large prime numbers p and q
- Obvious way:

```
Pick big number $x$
 for $i$ = 2 to sqrt ($x$)
     if $i$ divides $x$ its not prime,
         start over with $x$ + 1
done – $x$ is prime
```

How many prime numbers?

- Infinite (proved by Euclid, 300BC)
- Proof by contradiction:

Suppose that there exist only finitely many primes $\boldsymbol{p}_1 < \boldsymbol{p}_2 < ... < \boldsymbol{p}_r$.

Let $\mathbf{N} = (\boldsymbol{p}_1)(\boldsymbol{p}_2)...(\boldsymbol{p}_r) + 1$

$\mathbf{N} > \boldsymbol{p}_r$ so it is composite, $\mathrm{N} = p * \mathrm{M}$

If $\boldsymbol{p} = \boldsymbol{p}_\mathrm{i}$ for some $1 \ldots r$, then,

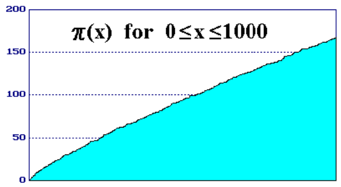
$\mathbf{N} = \boldsymbol{p}_\mathrm{i} * \boldsymbol{M} = \boldsymbol{p}_\mathrm{i} * (\boldsymbol{p}_1)(\boldsymbol{p}_2)...(\boldsymbol{p}_{i-1})(\boldsymbol{p}_{\mathrm{i}+1})...(\boldsymbol{p}_r) + 1$

$\boldsymbol{p}_\mathrm{i}\,(\boldsymbol{M} - (\boldsymbol{p}_1)(\boldsymbol{p}_2)...(\boldsymbol{p}_{i-1})(\boldsymbol{p}_{\mathrm{i}+1})...(\boldsymbol{p}_r)) = 1$

Contradiction: $\boldsymbol{p}_\mathrm{i} > 1$

Hence, there must be infinitely many primes.

Density of Primes



$\pi(x)$ is the number of primes $\leq x$

From http://www.utm.edu/research/primes/howmany.shtml

Approximating $\pi(x)$

- The Prime Number Theorem:

  $\pi(x) \sim x/\ln x$

- So, to find a prime bigger than x, we need to make about $\ln x/2$ guesses
- (Naïvely) Each guess requires sqrt(x) work
- For 200 digits (worst imaginable case):

  230 guesses * 10^{100}

- More work than breaking 3DES!

Need a faster prime test

- There are several fast probabilistic prime tests
- Can quickly test a prime with high probability, with a small amount of work
- If we pick a non-prime, its not a disaster (exercise for reader, will be on PS3)

Fermat Test

- Recall Fermat's Little Theorem: if n is prime and a is not divisible by n then $a^{n-1} \equiv 1 \bmod n$
- Prove n is composite by finding $a^{n-1} \not\equiv 1 \bmod n$
- Showing $a^{n-1} \equiv 1 \bmod n$ does **not** prove it is prime
- But if it holds for many a's it is **likely** than n is prime
  - Holds for all a's for some non-primes known as Carmichael Numbers: 561, 645, 1105, ...)

Properties of E and D

Trap-door one way function:

✓ 1. $D(E(M)) = M$

✓ 2. E and D are easy to compute.

3. Revealing E doesn't reveal an easy way to compute D

Trap-door one way permutation: also

➡ 4. $E(D(M)) = M$

Property 4: $E(D(M)) = M$

$$D(M) = M^d \bmod n$$
$$E(D(M)) = (M^d \bmod n)^e \bmod n$$
$$= M^{de} \bmod n$$
$$= M^{ed} \bmod n$$
$$= M$$

(from the property 1 proof)

Applications of RSA

- Privacy:
  - Bob encrypts message to Alice using E_A
  - Only Alice knows D_A
- Signatures:
  - Alice encrypts a message to Alice using D_A
  - Bob decrypts using E_A
  - Knows it was from Alice, since only Alice knows D_A
- Things you use every day: ssh, SSL, DNS, etc.

Two "Questionable" Statements in RSA Paper

1. "The need for a courier between every pair of users has thus been replaced by the requirement for a single secure meeting between each user and the public file manager when the user joins the system."

(p. 6)

Two "Questionable" Statements in RSA Paper

2. "(The NBS scheme (DES) is probably somewhat faster if special-purposed hardware encryption devices are used; our scheme may be faster on a general-purpose computer since multiprecision arithmetic operations are simpler to implement than complicated bit manipulations.)"

(p. 4)

Who *really* invented RSA?

- General Communications Headquarters, Cheltenham (formed from Bletchley Park after WWII)
- 1969 – James Ellis asked to work on key distribution problem
- Secure telephone conversations by adding "noise" to line
- Late 1969 – idea for PK, but function

RSA & Diffie-Hellman

- Asks Clifford Cocks, Cambridge mathematics graduate, for help
- He discovers RSA (four years early)
- Then (with Malcolm Williamson) discovered Diffie-Hellman
- Kept secret until 1997!
- NSA claims they had it even earlier

Charge

- Reread the parts of RSA paper you didn't understand the first time
- PS2 Due Weds

- Next time: security of RSA (third property)
  3. Revealing *E* doesn't reveal an easy way to compute *D*