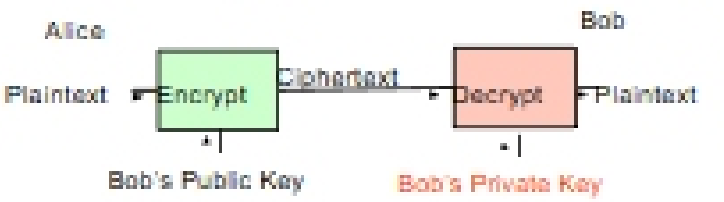
Lecture 8: Non-secret Key Cryptosystems (How Euclid, Fermat and Euler Created E-Commerce)

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.

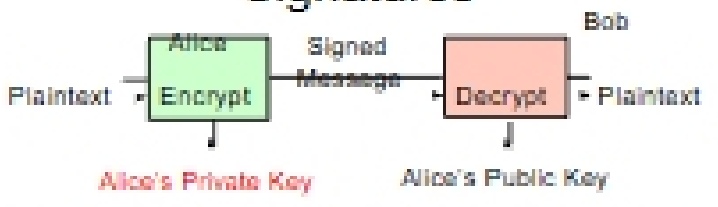
David Evans
http://www.cs.virginia.edu/~evans

Public-Key Applications: Privacy



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

Signatures



- 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: $E(D(m)) = D(E(m)) = m$
- 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

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

$$D(C) = C^d \bmod n \quad \text{(red = secret)}$$

$n = pq$ 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+/,
/dsM0<J]dsJxp"|dc`
```

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

(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

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

Totient Products

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

$\phi(n) = \phi(pq)$

$\phi(n)$ = 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

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

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

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

Euler's Theorem

- For a and n relatively prime:

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

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

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

Fermat's Little Theorem

If n is prime and a is not divisible by n

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

Stronger version: (in MBC p. 200):

If n is prime, for any a:

$$a^n \equiv a \bmod n$$

Fermat's Little Theorem Proof

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

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

and a is relatively prime to n

then $b = c \bmod n$

Fermat's Little Theorem Proof

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

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

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

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

Euler's Theorem

For a and n relatively prime:

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

Proof:

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

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

by Fermat's Little Theorem.

What if n is not prime?

Euler's Theorem, cont.

For a and n relatively prime:

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

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

We can write those numbers as:

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