Hardy's Mistake
The Unexpected Applicability of Pure Mathematics to Cryptography

Spring 1996 G. C. Steward Lectures
Gonville and Caius College

Whitfield Diffie
Sun Microsystems

8 March 1996

1

Public Key Cryptography

- Keys Come In Inverse Pairs
- Given One — Can't Find the Other

Public Key
— In telephone directory
Secret Key
— In subscriber's safe

2

Signed and Sealed Message

Sealed

$$\Big\{\{message\}^{\text{Sender Private Key}}, SenderID\Big\}^{\text{Receiver Public Key}}$$

Signed

3

RSA* System

$$Message \rightarrow Message^{e} \pmod{p \times q}$$

Public Key is Product $p \times q$

Secret Key is Factors: (p, q)

* Rivest, Shamir, and Adleman

4

Factors and Primes

- k is a *factor* of n if $\exists l$ such that $k \times l = n$
- k is a *proper factor* of n if k is a factor of n and k is neither 1 nor n.
- p is *prime* if and only if p has no proper factors.
- m and n are *relatively prime* if no number is a proper factor of both m and n.

5

Semi-groups and Groups

- *Closure*: $\forall x, y \in G : \; x \cdot y \in G$
- *Associativity*:

$$\forall x, y, z \in G : \; x \cdot (y \cdot z) = (x \cdot y) \cdot z.$$

- *Identity*: $\exists i \in G \,\mathbf{st}\, \forall x \in G : \; i \cdot x = x \cdot i = i$
- *Inverse*: $\forall x \in G, \exists y \in G \,\mathbf{st}\, x \cdot y = y \cdot x = i.$
- (sometimes) *Commutativity*: $\forall x, y \in G : \; x \cdot y = y \cdot x.$

6

Rings and Fields

Non-empty set R together with two binary operations $+$ and $\cdot$ such that:

- $(R, +)$ is a commutative group and $(R, \cdot)$ is a semi-group.
- Multiplication distributes over addition, that is $\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.
- *Field*: $(R - 0, \cdot)$ is a group.

7

Arithmetic Modulo n

For all n, the set $\{0, 1, 2, \ldots, n-1\}$ together with the addition operation $+$ forms a commutative group.

The set $\{1, 2, \ldots, n-1\}$ together with the multiplication operation $\times$ forms a group (also commutative) if and only if n is prime.

8

Arithmetic Modulo n (Cont'd)

If n is composite, there are non-invertible non-zero elements between 1 and $n-1$ called *zero divisors*, whose products with other non-zero elements is zero. In this case the set $\{1, 2, \ldots, n-1\}$ is not closed under multiplication.

9

Arithmetic Modulo n (Cont'd)

$$\mathcal{R} = \{0, \ldots, n-1\}$$

If $\mathcal{R} - \{0\}$ is a group (i.e., n is prime), $\mathcal{R}$ is called a field and denoted GF(n), otherwise $\mathcal{R}$ is called a ring.

The set of elements of $\mathcal{R} - \{0\}$ that is invertible forms a group called the *group of units of* $\mathcal{R}$.

10

Why is 1 Not a Prime

- Usual reason: convention for unique factorization.
- Better reason: 1 is a unit and factoring is meaningless in groups.

11

Zero Divisors

If x and y are non-zero elements of $\mathcal{R}$ such that:

$$x \cdot y = 1$$

then x and y are called *zero divisors*.

In a finite ring any element must be either a unit or a zero divisor.

12

Units Are Not Zero Divisors

If x is invertible, $\exists y$ s.t. x · y = 1. If x is a zero divisor then $\exists v \neq 0$ such that:

$$x \cdot v = 0$$

but then:

$$1 \cdot v = (x \cdot y) \cdot v = (y \cdot x) \cdot v = y \cdot (x \cdot v) = y \cdot 0 = 0$$

so $1 \cdot v = 0$ or $v = 0$. Oops!

13

Non-units are Zero Divisors

Suppose $0 \neq m \in Z_n$ is not invertible. Then:

$$1 \cdot m \neq 1$$
$$2 \cdot m \neq 1$$
$$\vdots$$
$$(n-1) \cdot m \neq 1$$

so since $1 \cdot m \cdots (n-1) \cdot m$ all fall in the set $\underbrace{Z_n - \{0, 1\}}_{n-2 \text{ elements}}$

14

Non-units are Zero Divisors (Cont'd)

There must be distinct k and $\ell \in \{2, \ldots, \text{n}-1\}$ s.t.

$$k \cdot m = \ell \cdot m$$

i.e.,

$$k \cdot m - \ell \cdot m = 0 \Longrightarrow (k - \ell) \cdot m = 0,$$

but since $k \neq \ell$, $k - l \neq 0$ and m must be a zero divisor.

15

Invertible Elements Modulo n

Theorem: The invertible elements of $\mathcal{R}$ are the elements relatively prime to n.

Proof: Let $\gcd(m, n) = k$. If $k > 1$ then $\frac{n}{k} < n$ and not congruent to zero modulo n, but

$$m \cdot \frac{n}{k} = \frac{m}{k} \cdot n$$

a multiple of n, and thus congruent to zero, making m a zero divisor, modulo n.

16

Euler's Totient Function ϕ

The Euler *Totient* function is the size of the group of units modulo n. I.e., it is the number of positive integers less than n and relatively prime to n.

17

Example: $\phi(33) = \phi(3 \times 11) = 2 \times 10 = 20$

1√	8√	15	22	29√
2√	9	16√	23√	30
3	10√	17√	24	31√
4√	11	18	25√	32√
5√	12	19√	26√	33
6	13√	20√	27	
7√	14√	21	28√	

18

The Euler ϕ-Function (cont'd)

$$\begin{aligned}
\mathrm{U}(\mathrm{Z}_1) &= \{1\} \quad \phi(1) = 1 \\
\mathrm{U}(\mathrm{Z}_2) &= \{1\} \quad \phi(2) = 1 \\
\mathrm{U}(\mathrm{Z}_3) &= \{1,2\} \quad \phi(3) = 2 \\
\mathrm{U}(\mathrm{Z}_4) &= \{1,3\} \quad \phi(4) = 2 \\
\mathrm{U}(\mathrm{Z}_5) &= \{1,2,3,4\} \quad \phi(5) = 4 \\
\mathrm{U}(\mathrm{Z}_6) &= \{1,5\} \quad \phi(6) = 2 \\
\mathrm{U}(\mathrm{Z}_7) &= \{1,2,3,4,5,6\} \quad \phi(7) = 6 \\
\mathrm{U}(\mathrm{Z}_8) &= \{1,3,5,7\} \quad \phi(7) = 4
\end{aligned}$$

19

Important Cases of $\phi(n)$

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

$$\begin{aligned}
\phi(p \times q) &= (p \times q) \\
&\quad - p \quad \text{multiples of } q \\
&\quad - q \quad \text{multiples of } p \\
&\quad + 1 \quad \text{counted } p \times q \text{ twice} \\
&= p \times q - p - q + 1 \\
&= (p-1)(q-1)
\end{aligned}$$

20

Orbit of a Unit

Let $x \in U(Z_n)$, the group of units of Z_n and consider

$$x \; x^2 \; x^3 \; x^4 \; \cdots$$

The map $\bullet_x : U(\mathrm{Z}_n) \to U(\mathrm{Z}_n) : w \mapsto w \cdot x$ is invertible, so these all lie on one cycle.

21

The Subgroup Generated by x

The powers $x, x^2, \cdots, x^{k-1}$ form a subgroup of order k of $\mathrm{U}(\mathrm{Z}_n)$ and so

$$k | \#(\mathrm{U}(\mathrm{Z}_n)) = \phi(n).$$

Therefore

$$x^{\phi(n)} = (x^k)^{\frac{\phi(n)}{k}} = 1.$$

22

$\exists \ell$ such that $x^\ell = x$

This means there is some ℓ such that $x^\ell = x$. Call $\ell - 1$, k. Then $x, x^2, \cdots, x^k$ are the k powers of x. Furthermore, $x^k = \frac{x^\ell}{x} = \frac{x}{x} = 1$.

23

Euler's Theorem — 1761*

$\forall_{x \in \mathrm{U}(\mathrm{Z}_n)}$ $(0 < x < n$ and $\gcd(x, n) = 1)$,

$$x^{\phi(n)} \equiv 1 \pmod{n}.$$

Corollary:

$$\forall_{0 \le x < n}, \; x^{k \times \phi(n)+1} \equiv x \pmod{n}.$$

* Navi Comm Ac Petrop 8 1760–1 p. 74 Comm Arith 1. 272–286 2. 524–6.

24

Decryption in RSA

Given a Cryptogram: M^{e}

$$\mathrm{ET} \Longrightarrow \forall_{0 \leq x < n},\ x^{k \times \phi(n)+1} \equiv x \pmod{n}$$

Choose d so that $\mathrm{d} \times \mathrm{e} \equiv 1 \pmod{\phi(n)}$ then:

$$(\mathrm{M}^{\mathrm{e}})^{\mathrm{d}} \equiv M^{\mathrm{e} \times \mathrm{d}} \equiv \mathrm{M}^{k \times \phi(n)+1} \equiv \mathrm{M}$$

25

Example: $n = 3 \times 11 = 33$

Suppose M = 2 and e = 3

Encrypt: $2^3 = 8$

$$3 \times 7 = 21 \equiv 1 \pmod{\phi(33)} \Longrightarrow e = 7$$

Decrypt: $8^7 = 2^{21} \equiv 2 \pmod{33}$

26

Certificates

A *certificate* is a signed message containing a public key together with information identifying the holder of the corresponding private key.

27

Exponential Key Agreement

Choose a large prime P and a primitive element α in arithmetic modulo P (I.e., $\forall_{0<n<P} \exists k$ such that $\alpha^k = n \pmod{P}$ or the α^n generate all non-zero elements of GF(P).)

For any $x \in \mathrm{GF}(P)$ calculating $\alpha^x \bmod P$ is easy, but given that $\alpha^x = y \pmod{P}$, finding $x = \log_\alpha \pmod{P}$ is hard.

28

Exponential Key Agreement (Cont'd)

A and B want to communicate.

A generates x at random and sends α^x to B.
B generates y at random and sends α^y to A.
A calculates $(\alpha^y)^x = \alpha^{xy}$.
B calculates $(\alpha^x)^y = \alpha^{xy}$.
A and B now both know α^{xy}.

29

Key Exchange with Certificates

A. Alice and Bob do exponential key exchange.
B. Alice and Bob exchange certificates and each check the system signature on the other's certificate.
C. Alice signs the α^y she got from Bob and Bob signs the α^x he got from Alice.

30