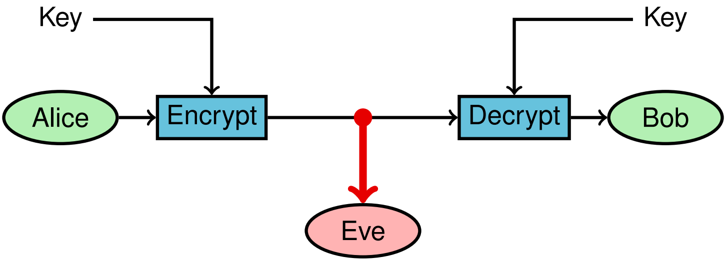
Cryptography Lecture 6

Public key principles, one-way functions, RSA

LINKÖPING
UNIVERSITY

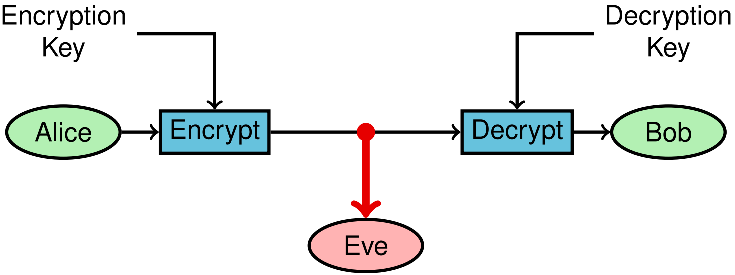
Symmetric key cryptography

Thus far in the course, we have learnt about systems where the encryption key is the same as the decryption



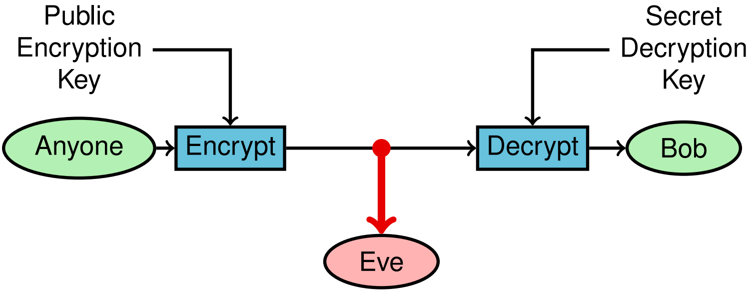
Asymmetric key cryptography

In 1976, Diffie and Hellman proposed the use of different keys for encryption and decryption



Public key cryptography

Asymmetric key systems can be used in public key cryptography



One-way functions

A one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate $f(x)$ from x
- Hard to invert: to calculate x from $f(x)$

There is no proof that one-way functions exist, or even real evidence that they can be constructed

Even so, there are examples that seem one-way: they are easy to compute but we know of no easy way to reverse them, for example

$$x^2 \text{ is easy to compute mod } n = pq \text{ but } x^{1/2} \text{ is not}$$

One-way function candidate: modular exponentiation

A one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)

Example: $2^{1233} \bmod 789$

n	$2^n \bmod 789$
2	4
4	16
8	256
16	65536=49
32	34
64	367
128	559
256	37
512	580
1024	286

$$2^{1233} = 2^{1024}2^{128}2^{64}2^{16}2^{1} = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 2 = 635 \bmod 789$$

Trapdoor one-way functions

A one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate $f(x)$ from x
- Hard to invert: to calculate x from $f(x)$

A *trapdoor* one-way function has one more property, that with certain knowledge it *is* easy to invert, to calculate x from $f(x)$

There is no proof that trapdoor one-way functions exist, or even real evidence that they can be constructed.

A few examples will follow (anyway)

Trapdoor one-way function candidate: modular exponentiation

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

$$2^{1233} = 635 \bmod 789$$
$$635^{17} = 2 \bmod 789$$

There is no proof that this is a true trapdoor one-way function, but we think it is

Trapdoor one-way function candidate: modular exponentiation

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

$$2^{1233} = 635 \bmod 789$$
$$635^{17} = 2 \bmod 789$$

There is no proof that this is a true trapdoor one-way function, but we think it is

Mathematical requirements

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

$$x^{1233} = y \bmod 789$$
$$y^{17} = x \bmod 789$$

Somehow, $(x^{1233})^{17} = x^{1233 \cdot 17} = x^1 \bmod 789$, that is, $1233 \cdot 17 = 1$ in the exponent. Why and how do we find the numbers?

Greatest Common Divisor

$$\gcd(576, 135) =$$

Greatest Common Divisor

$$\gcd(576, 135) = \gcd(135, 36)$$

The Euclidean algorithm

$$576 = 4 \cdot 135 + 36$$

Greatest Common Divisor

$$\mathrm{gcd}(576, 135) = \mathrm{gcd}(135, 36) = \mathrm{gcd}(36, 27)$$

The Euclidean algorithm

$$576 = 4 \cdot 135 + 36$$
$$135 = 3 \cdot 36 + 27$$

Greatest Common Divisor

$$\gcd(576, 135) = \gcd(135, 36) = \gcd(36, 27) = \gcd(27, 9)$$

The Euclidean algorithm

$$\begin{aligned} 576 &= 4 \cdot 135 + 36 \\ 135 &= 3 \cdot 36 + 27 \\ 36 &= 1 \cdot 27 + 9 \end{aligned}$$

Greatest Common Divisor

$$\gcd(576, 135) = \gcd(135, 36) = \gcd(36, 27) = \gcd(27, 9) = 9$$

The Euclidean algorithm

$$\begin{aligned} 576 &= 4 \cdot 135 + 36 \\ 135 &= 3 \cdot 36 + 27 \\ 36 &= 1 \cdot 27 + 9 \\ 27 &= 3 \cdot 9 + 0 \end{aligned}$$

Greatest Common Divisor

Theorem (the extended Euclidean algorithm): Given nonzero a and b, there exist x and y such that

$$ax + by = \gcd(a, b)$$

A proof is available in the book. Outline:

$$\begin{aligned}
576 &= 4 \cdot 135 + 36 \\
135 &= 3 \cdot 36 + 27 \\
36 &= 1 \cdot 27 + 9 \\
27 &= 3 \cdot 9 + 0
\end{aligned}$$

Greatest Common Divisor

Theorem (the extended Euclidean algorithm): Given nonzero a and b, there exist x and y such that

$$ax + by = \gcd(a, b)$$

A proof is available in the book. Outline:

$$\begin{aligned} 576 &= 4 \cdot 135 + 36 \\ 135 &= 3 \cdot 36 + 27 \\ 36 &= 1 \cdot 27 + 9 \\ 27 &= 3 \cdot 9 + 0 \end{aligned}$$

$$9 = 36 - 1 \cdot 27$$

Greatest Common Divisor

Theorem (the extended Euclidean algorithm): Given nonzero a and b, there exist x and y such that

$$ax + by = \gcd(a, b)$$

A proof is available in the book. Outline:

$$\begin{aligned} 576 &= 4 \cdot 135 + 36 \\ 135 &= 3 \cdot 36 + 27 \\ 36 &= 1 \cdot 27 + 9 \\ 27 &= 3 \cdot 9 + 0 \end{aligned}$$

$$\begin{aligned} 27 &= 135 - 3 \cdot 36 \\ 9 &= 36 - 1 \cdot 27 \end{aligned}$$

Greatest Common Divisor

Theorem (the extended Euclidean algorithm): Given nonzero a and b, there exist x and y such that

$$ax + by = \gcd(a, b)$$

A proof is available in the book. Outline:

$$\begin{aligned} 576 &= 4 \cdot 135 + 36 \\ 135 &= 3 \cdot 36 + 27 \\ 36 &= 1 \cdot 27 + 9 \\ 27 &= 3 \cdot 9 + 0 \end{aligned}$$

$$\begin{aligned} 36 &= 576 - 4 \cdot 135 \\ 27 &= 135 - 3 \cdot 36 \\ 9 &= 36 - 1 \cdot 27 \end{aligned}$$

Greatest Common Divisor

Theorem (the extended Euclidean algorithm): Given nonzero a and b, there exist x and y such that

$$ax + by = \gcd(a, b)$$

A proof is available in the book. Outline:

$$\begin{aligned}
576 &= 4 \cdot 135 + 36 \\
135 &= 3 \cdot 36 + 27 \\
36 &= 1 \cdot 27 + 9 \\
27 &= 3 \cdot 9 + 0
\end{aligned}$$

$$\begin{aligned}
36 &= 576 - 4 \cdot 135 \\
27 &= 135 - 3 \cdot 36 \\
9 &= 36 - 1 \cdot 27
\end{aligned}$$

$$\begin{aligned}
9 = 36 - 27 = 36 - (135 - 3 \cdot 36) &= -135 + 4 \cdot 36 \\
= -135 + 4 \cdot (576 - 4 \cdot 135) &= 4 \cdot 576 - 17 \cdot 135
\end{aligned}$$

Arithmetic mod n

- Numbers mod n are equal (congruent) if their difference is a multiple of n
- Addition, subtraction, and multiplication mod n works as usual:

$$5 = 27 \text{ mod } 11 \quad \text{because } 27 - 5 = 2 \cdot 11$$

$$\begin{aligned} 5 + 7 &= 1 \text{ mod } 11 && \text{because } (5 + 7) - 1 = 11 \\ 5 - 7 &= 9 \text{ mod } 11 && \text{because } 9 - (5 - 7) = 11 \\ 5 \cdot 7 &= 2 \text{ mod } 11 && \text{because } (5 \cdot 7) - 2 = 3 \cdot 11 \end{aligned}$$

- But division is not always possible

Division mod n

If $\gcd(a, n) = 1$, then you can divide by a, because of the following theorem:

Theorem: If $\gcd(a, n) = 1$ there exists an x such that $ax = 1 \bmod n$

Proof: The extended Euclidean algorithm gives us x and y so that $ax + ny = 1$. Now,

$$ax + ny = ax \bmod n$$

so

$$ax = 1 \bmod n$$

Division mod n

Example: solve

$$\begin{aligned} 5x + 6 &= 2 \bmod 11 \\ 5x &= -4 \bmod 11 \end{aligned}$$

Division by 5 is possible because $\gcd(5, 11) = 1$, and the extended Euclidean algorithm gives $-2 \cdot 5 + 1 \cdot 11 = 1$ so that $-2 = 1/5$ mod 11.

$$\begin{aligned} 5x &= 7 \bmod 11 \\ -2 \cdot 5x &= -2 \cdot 7 \bmod 11 \\ x &= -14 \bmod 11 \\ x &= 8 \bmod 11 \end{aligned}$$

Division mod n

Example: solve

$$\begin{aligned} 5x + 6 &= 2 \bmod 12 \\ 5x &= -4 \bmod 12 \end{aligned}$$

Division by 5 is possible because $\gcd(5, 12) = 1$, and the extended Euclidean algorithm gives $-7 \cdot 5 + 3 \cdot 12 = 1$ so that $-7 = 1/5$ mod 12.

$$\begin{aligned} 5x &= 8 \bmod 12 \\ -7 \cdot 5x &= -7 \cdot 8 \bmod 12 \\ x &= -56 \bmod 12 \\ x &= 4 \bmod 12 \end{aligned}$$

Division mod n

Example: solve

$$5x + 6 = 2 \text{ mod } 10$$

Division by 5 is not possible because $\gcd(5, 10) = 5$.

- If x is odd, the left-hand side is odd while the right-hand side is even, so no solutions.
- If x is even, the left-hand side is 6 (mod 10, whatever value x has), and the right-hand side is 2 (mod 10), so no solutions

Division mod n

Example: solve

$$6x + 6 = 2 \text{ mod } 10$$

Division by 6 is not possible because $\gcd(6, 10) = 2$.

And yet there are solutions, because all terms have a factor 2. In this case, you should solve the reduced congruence

$$3x + 3 = 1 \text{ mod } 5,$$

Division with 3 (multiplication with 2) gives

$$x + 1 = 2 \text{ mod } 5,$$

so that $x = 1$ is the solution. The original equation has the solutions 1 and 6, both $= 1$ mod 5

Division mod n

Division by 5 mod 11 is possible because $\gcd(5, 11) = 1$, and the extended Euclidean algorithm gives $-2 \cdot 5 + 1 \cdot 11 = 1$ so that $-2 = 1/5$ mod 11.

Division by 5 mod 12 is possible because $\gcd(5, 12) = 1$, and the extended Euclidean algorithm gives $-7 \cdot 5 + 3 \cdot 12 = 1$ so that $-7 = 1/5$ mod 12.

Division by 5 mod 10 is not possible because $\gcd(5, 10) = 5$.

OK. But we want to divide in the exponent:

$$x^{1233 \cdot 17} = x^1 \bmod 789$$

Fermat's little theorem

Having learnt how division works (mod p), we can prove

Theorem: If p is a prime and p does not divide a, then $a^{p-1} = 1$ mod p

Proof: Since p does not divide a, a^{-1} exists mod p, which means that multiplication with a is one-to-one. Then

$$(a \cdot 1)(a \cdot 2)...(a \cdot (p-1)) = 1 \cdot 2 \cdot ... \cdot (p-1) \text{ mod } p$$

and since p does not divide $1 \cdot 2 \cdot ... \cdot (p-1)$, we can divide with the right-hand side and obtain the congruence of the theorem

Fermat's little theorem

Having learnt how division works (mod p), we can prove

Theorem: If p is a prime and p does not divide a, then $a^{p-1} = 1 \bmod p$

Proof: Since p does not divide a, a^{-1} exists mod p, which means that multiplication with a is one-to-one. Then

$$(a \cdot 1)(a \cdot 2)...(a \cdot (p-1)) = 1 \cdot 2 \cdot ... \cdot (p-1) \bmod p$$

and since p does not divide $1 \cdot 2 \cdot ... \cdot (p-1)$, we can divide with the right-hand side and obtain the congruence of the theorem

Example: $3^4 = 1 \bmod 5$; $\quad 33^{42} = 1 \bmod 43$

Fermat's little theorem, again

Having learnt how division works (mod p), we can prove

Theorem: If p is a prime and p does not divide a, then $a^{p-1} = 1 = a^0$ mod p

In other words: Calculations that are mod p in the base number are mod $p-1$ in the exponent

Example:

$$3^4 = 1 \bmod 5,\ 3^5 = 3 \bmod 5;$$
$$33^{42} = 1 \bmod 43,\ 33^{43} = 33 \bmod 43$$

Trapdoor one-way function candidate: exponentiation modulo a prime p?

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod p$) from x
- Hard to invert: to calculate x from ($x^e \bmod p$)?

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod p)^d \bmod p$

Calculations in the exponent are mod $p - 1$, so we need $ed = 1 \bmod p - 1$

Unfortunately, the extended Euclidean algorithm is an efficient algorithm to find d. This is not good enough.

Trapdoor one-way function candidate: modular exponentiation

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)?

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

What about composite n?

Euler's theorem

Having learnt how division works (mod n), we can prove

Theorem: If $\gcd(a, n) = 1$, then

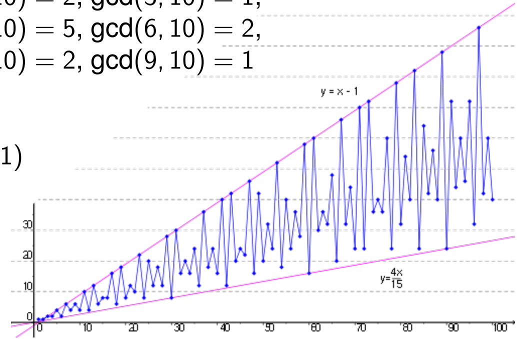
$$a^{\phi(n)} = 1 \bmod n,$$

where $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

Euler's totient function $\phi(n)$

Euler's totient function $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

- $\phi(p) = p - 1$ if p is prime
- $\phi(10) = 4$ because $\gcd(1, 10) = 1$, $\gcd(2, 10) = 2$, $\gcd(3, 10) = 1$, $\gcd(4, 10) = 2$, $\gcd(5, 10) = 5$, $\gcd(6, 10) = 2$, $\gcd(7, 10) = 1$, $\gcd(8, 10) = 2$, $\gcd(9, 10) = 1$
- $\phi(pq) = (p - 1)(q - 1)$
- $\phi(p^2 q) = p(p - 1)(q - 1)$



Euler's theorem

Having learnt how division works (mod n), we can prove

Theorem: If $\gcd(a, n) = 1$, then

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

where $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

Proof: Since $\gcd(a, n) = 1$, a^{-1} exists mod n, which means that multiplication with a is one-to-one. For the integers $1 \leq x_i \leq n$ such that $\gcd(x_i, n) = 1$, it holds that $\gcd(ax_i, n) = 1$, so

$$(a \cdot x_1)(a \cdot x_2) \cdot \ldots \cdot (a \cdot x_{\phi(n)}) = x_1 x_2 \cdot \ldots \cdot x_{\phi(n)} \bmod n$$

and since $\gcd(x_1 x_2 \ldots x_{\phi(n)}, n) = 1$, we can divide with the right-hand side and obtain the congruence of the theorem

LINKÖPING UNIVERSITY

Euler's theorem, again

Having learnt how division works (mod n), we can prove

Theorem: If $\gcd(a, n) = 1$, then

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

where $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

In other words: Calculations that are mod n in the base number are mod $\phi(n)$ in the exponent

Example:

$$x^{1233 \cdot 17} = x^1 \bmod 789 = 263 \times 3, \text{ because}$$
$$1233 \cdot 17 = 1 \bmod 524 = \phi(789) = 262 \times 2,$$

Trapdoor one-way function candidate: modular exponentiation

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)?

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

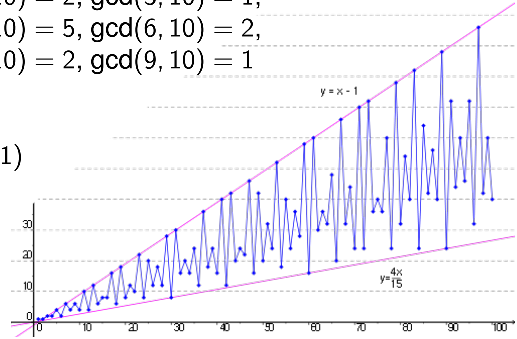
Calculations in the exponent are mod $\phi(n)$, so we need $ed = 1 \bmod \phi(n)$

The extended Euclidean algorithm is an efficient algorithm to find d, but you need to know $\phi(n)$, otherwise it won't work!

Euler's totient function $\phi(n)$

Euler's totient function $\phi(n)$ is the number of integers $1 \leq x \leq n$ such that $\gcd(x, n) = 1$

- $\phi(p) = p - 1$ if p is prime
- $\phi(10) = 4$ because
  $\gcd(1, 10) = 1$, $\gcd(2, 10) = 2$, $\gcd(3, 10) = 1$,
  $\gcd(4, 10) = 2$, $\gcd(5, 10) = 5$, $\gcd(6, 10) = 2$,
  $\gcd(7, 10) = 1$, $\gcd(8, 10) = 2$, $\gcd(9, 10) = 1$
- $\phi(pq) = (p - 1)(q - 1)$
- $\phi(p^2q) = p(p - 1)(q - 1)$



Trapdoor one-way function candidate: exponentiation modulo $n = pq$

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate ($x^e \bmod n$) from x
- Hard to invert: to calculate x from ($x^e \bmod n$)?

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

Euler's theorem tells us that if we use $n = pq$, and *know the factorization*, we can calculate $\phi(n) = \phi(pq) = (p-1)(q-1)$ and also d.

OK, so we use a large composite $n = pq$ that cannot be factored efficiently

Trapdoor one-way function candidate: exponentiation modulo $n = pq$

Euler's theorem tells us that if we use $n = pq$, and *know the factorization*, we can calculate $\phi(n) = \phi(pq) = (p-1)(q-1)$ and also d.

But that is only *one possible method*. Perhaps there are others?

How hard is it to solve for x in

$$x^e = c \bmod n?$$

We will see that it is equally hard as factoring $n = pq$

Square roots mod n

$x^2 = 1$ mod 7 has the solutions ± 1 (as for all odd primes)

$x^2 = 1$ mod 15 has the solutions ± 1, ± 4

The last seems simple enough (± 1 mod 3 and ± 1 mod 5), but how do we find solutions in general?

Chinese remaindering

Example:

$$x = 25 \bmod 42 \Rightarrow \begin{cases} x = 4 \bmod 7 \\ x = 1 \bmod 6 \end{cases}$$

Chinese remaindering

Example:

$$x = 25 \bmod 42 \Rightarrow \begin{cases} x = 4 \bmod 7 \\ x = 1 \bmod 6 \end{cases}$$

Chinese remainder theorem:

$$x = 25 \bmod 42 \Leftarrow \begin{cases} x = 4 \bmod 7 \\ x = 1 \bmod 6 \end{cases}$$

Chinese remaindering

Theorem: Suppose $\gcd(n, m) = 1$. Given integers a and b, there exists exactly one solution x mod mn to the simultaneous congruences

$$\begin{cases} x = a \bmod m \\ x = b \bmod n \end{cases}$$

Proof: The extended Euclidean algoritm gives us s and t such that $ms + nt = 1$, or

$$ms = 1 \bmod n \quad \text{and} \quad nt = 1 \bmod m.$$

The number $x = bms + ant$ is a solution because

$$x = bms = b \bmod n \quad \text{and} \quad x = ant = a \bmod m.$$

If y is another solution, then $x = y$ mod n and $x = y$ mod m, so $x = y$ mod mn.

Square roots mod 15

Example: Solve $x^2 = 1 \bmod 15$.

- Break the congruence into two congruences over prime powers, since this is easier to solve
- Combine the solutions through Chinese remaindering

$x^2 = 1 \bmod 3$ has solutions $x = \pm 1 \bmod 3$
$x^2 = 1 \bmod 5$ has solutions $x = \pm 1 \bmod 5$

In total four combinations

$x = +1 \bmod 3$, $x = +1 \bmod 5$ gives $x = +1 \bmod 15$
$x = +1 \bmod 3$, $x = -1 \bmod 5$ gives $x = +4 \bmod 15$
$x = -1 \bmod 3$, $x = +1 \bmod 5$ gives $x = -4 \bmod 15$
$x = -1 \bmod 3$, $x = -1 \bmod 5$ gives $x = -1 \bmod 15$

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$x = +a \bmod pq$ gives $x = +a \bmod p$ and $x = +a \bmod q$
$x = -a \bmod pq$ gives $x = -a \bmod p$ and $x = -a \bmod q$
$x = +b \bmod pq$ gives $x = +b \bmod p$ and $x = +b \bmod q$
$x = -b \bmod pq$ gives $x = -b \bmod p$ and $x = -b \bmod q$

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$x = +a \bmod pq$ gives $x = +a \bmod p$ and $x = +a \bmod q$
$x = -a \bmod pq$ gives $x = -a \bmod p$ and $x = -a \bmod q$
$x = +b \bmod pq$ gives $x = +b \bmod p$ and $x = +b \bmod q$
$x = -b \bmod pq$ gives $x = -b \bmod p$ and $x = -b \bmod q$

- This means that $a = b \bmod p$ or $a = -b \bmod p$

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$$
\begin{aligned}
x = +a \bmod pq &\text{ gives } x = +a \bmod p \text{ and } x = +a \bmod q \\
x = -a \bmod pq &\text{ gives } x = -a \bmod p \text{ and } x = -a \bmod q \\
x = +b \bmod pq &\text{ gives } x = +b \bmod p \text{ and } x = +b \bmod q \\
x = -b \bmod pq &\text{ gives } x = -b \bmod p \text{ and } x = -b \bmod q
\end{aligned}
$$

- This means that $a = b \bmod p$ or $a = -b \bmod p$
- If $a = b \bmod p$ then $a = -b \bmod q$

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$x = +a \bmod pq$ gives $x = +a \bmod p$ and $x = +a \bmod q$
$x = -a \bmod pq$ gives $x = -a \bmod p$ and $x = -a \bmod q$
$x = +b \bmod pq$ gives $x = +b \bmod p$ and $x = +b \bmod q$
$x = -b \bmod pq$ gives $x = -b \bmod p$ and $x = -b \bmod q$

- This means that $a = b \bmod p$ or $a = -b \bmod p$
- If $a = b \bmod p$ then $a = -b \bmod q$, in other words p divides $a - b$ while q does not

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$$\begin{aligned}
x = +a \bmod pq &\text{ gives } x = +a \bmod p \text{ and } x = +a \bmod q\\
x = -a \bmod pq &\text{ gives } x = -a \bmod p \text{ and } x = -a \bmod q\\
x = +b \bmod pq &\text{ gives } x = +b \bmod p \text{ and } x = +b \bmod q\\
x = -b \bmod pq &\text{ gives } x = -b \bmod p \text{ and } x = -b \bmod q
\end{aligned}$$

- This means that $a = b \bmod p$ or $a = -b \bmod p$
- If $a = b \bmod p$ then $a = -b \bmod q$, in other words p divides $a - b$ while q does not, so that $\gcd(a - b, n) = p$ and we have factored n

Square roots mod pq

If we can solve $x^2 = y \bmod pq$, there will be four different solutions, $\pm a$ and $\pm b$, which will simultaneously solve $x^2 = y \bmod p$ and $x^2 = y \bmod q$:

$x = +a \bmod pq$ gives $x = +a \bmod p$ and $x = +a \bmod q$
$x = -a \bmod pq$ gives $x = -a \bmod p$ and $x = -a \bmod q$
$x = +b \bmod pq$ gives $x = +b \bmod p$ and $x = +b \bmod q$
$x = -b \bmod pq$ gives $x = -b \bmod p$ and $x = -b \bmod q$

- This means that $a = b \bmod p$ or $a = -b \bmod p$
- If $a = b \bmod p$ then $a = -b \bmod q$, in other words p divides $a - b$ while q does not, so that $\gcd(a - b, n) = p$ and we have factored n
- If $a = -b \bmod p$ then $a = b \bmod q$, then $\gcd(a - b, n) = q$

Trapdoor one-way function candidate: exponentiation modulo $n = pq$

A trapdoor one-way function is a function that is easy to compute but computationally hard to reverse

- Easy to calculate (x^e mod n) from x
- Hard to invert: to calculate x from (x^e mod n)?

The trapdoor is that with another exponent d it *is* easy to invert, to calculate $x = (x^e \bmod n)^d \bmod n$

We have shown (using the Chinese remainder theorem) that solving $x^2 = c \bmod pq$, obtaining four roots $\pm a \neq \pm b$, is equally hard as factoring $n = pq$.

Rivest Shamir Adleman (1977)

- Bob chooses secret primes p and q, and sets $n = pq$
- Bob chooses e with $\gcd(e, \phi(n)) = 1$
- Bob computes d so that $de = 1 \bmod \phi(n)$
- Bob makes n and e public but keeps p, q and d secret
- Alice encrypts m as $c = m^e \bmod n$
- Bob decrypts c as $m = c^d \bmod n$

Choose p and q: Test for primality

Theorem (Fermat's little theorem): If n is prime and $a \neq 0 \bmod n$, then $a^{n-1} = 1 \bmod n$

Fermat primality test: To test n, take a random $a \neq 0, \pm 1 \bmod n$. If $a^{n-1} \neq 1$, then n is composite, otherwise n is prime with high probability

Choose p and q: Test for primality

Theorem (Fermat's little theorem): If n is prime and $a \neq 0 \bmod n$, then $a^{n-1} = 1 \bmod n$

Fermat primality test: To test n, take a random $a \neq 0, \pm 1 \bmod n$. If $a^{n-1} \neq 1$, then n is composite, otherwise n is prime with high probability

How high? — We'll use a more advanced test

Choose p and q: Test for primality

Miller-Rabin primality test: To test n, take a random $a \neq 0, \pm 1 \bmod n$, and write $n - 1 = 2^k m$ with m odd

- Let $b_0 = a^m$, if this is ± 1 then stop: n is probably prime
- Let $b_{j+1} = b_j^2$, if this is $+1$ then stop: n is composite,
  if this is -1 then stop: n is probably prime
- Repeat. If you reach b_k then n is composite

(Seems complicated? Let's try to understand how it works...)

Choose p and q: Test for primality

Miller-Rabin primality test: To test n, take a random $a \neq 0, \pm 1 \bmod n$, and write $n - 1 = 2^k m$ with m odd

- Let $b_0 = a^m$, if this is ± 1 then stop: n is probably prime
  (because $a^{n-1} = 1$, remember the Fermat primality test)
- Let $b_{j+1} = b_j^2$, if this is $+1$ then stop: n is composite,
  (because $b_j \neq \pm 1$, so we can factor n)
  if this is -1 then stop: n is probably prime
  (because $a^{n-1} = 1$, Fermat again)
- Repeat. If you reach b_k then n is composite
  (if $b_k = +1$ remember that $b_{k-1} \neq \pm 1$ so we can factor n,
  otherwise $b_k = a^{n-1} \neq 1$, remember the Fermat primality test)

Choose p and q: Only test for primality

- Both the Fermat test and the Miller-Rabin test (and the Solovay-Strassen test in the book) are probabilistic tests.
- They are fast but can fail, the Miller-Rabin test fails with probability less than 1/4 (bad value of a). Performing the test for say 10 different random values of a will fail once in a million.
- The primality test from 2004 by Agrawal, Kayal and Saxena is deterministic and polynomial time (efficient), but can nevertheless still not compete with the probabilistic tests

Choose p and q: Avoid simple factorization

- The **Fermat factorization method** uses
  $n = x^2 - y^2 = (x + y)(x - y)$
- Calculate $n + 1^2$, $n + 2^2$, $n + 3^2$, $n + 4^2$, $n + 5^2$, $\ldots$, until we reach a square, then we are done.

  Example:

$$295927 + 3^2 = 295936 = 544^2$$
$$295927 = 544^2 - 3^2 = 541 \cdot 547$$

- This is unlikely to be a problem for a many-digit $n = pq$, but usually p and q are chosen to be of slightly different size, to be on the safe side

Choose p and q: Avoid simple factorization

The **Pollard** $p - 1$ **factorization** method uses $b = a^{B!} \bmod n$ for chosen a and B. Calculate $d = \gcd(b - 1, n)$. If d is not 1 or n, we have factored n.

This works if one prime factor p of n is such that $p - 1$ has only small factors. If B is big enough, $B! = k(p - 1)$, and $b = a^{B!} = 1 \bmod p$ Then, $b - 1$ contains a factor p, as does n.

Solution: choose p and q so that $p - 1$ and $q - 1$ has at least one large prime factor

Choose p and q: Test for primality

Fermat primality test: Take a random $a \neq 0, \pm 1 \bmod n$.
If $a^{n-1} \neq 1$, then n is composite, otherwise n is prime with high probability

Miller-Rabin primality test: Take a random $a \neq 0, \pm 1 \bmod n$, and write $n - 1 = 2^k m$ with m odd

- Let $b_0 = a^m$, if this is ± 1 then stop: n is probably prime
- Let $b_{j+1} = b_j^2$, if this is $+1$ then stop: n is composite,
  if this is -1 then stop: n is probably prime
- Repeat. If you reach b_k then n is composite

Choose p and q: Avoid simple factorization

The **Fermat factorization method** works if p and q are close, so that trying $n^2 + 1^2$, $n^2 + 2^2$, $n^2 + 3^2$, ... will find a square in a reasonable amount of time

Solution: choose p and q to be of slightly different size

The **Pollard $p - 1$ factorization method** works if one prime factor p of n is such that $p - 1$ has only small factors

Solution: choose p and q so that $p - 1$ and $q - 1$ has at least one large prime factor

Rivest Shamir Adleman (1977)

- Bob chooses secret primes p and q, and sets $n = pq$
  - Choose primes p and q using, say, the Miller-Rabin test
  - Choose primes of slightly different size
  - Choose p and q so that $p - 1$ and $q - 1$ has at least one large prime factor
- Bob chooses e with $\gcd(e, \phi(n)) = 1$
- Bob computes d so that $de = 1 \bmod \phi(n)$
- Bob makes n and e public but keeps p, q and d secret
- Alice encrypts m as $c = m^e \bmod n$
- Bob decrypts c as $m = c^d \bmod n$