

Mathematics of Cryptography

Number Theory

Modular Arithmetic:

Two numbers **equivalent** mod n if their difference is multiple of n

example: 7 and 10 are equivalent mod 3 but not mod 4

$$7 \bmod 3 \equiv 10 \bmod 3 = 1; 7 \bmod 4 = 3, 10 \bmod 4 = 2.$$

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Look at the applet

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

$$\text{Ex: } 3^{(5-1)} = 81 = 1 \pmod{5}$$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots
Solve $x^2 = a \pmod{p}$ where p is a prime number.

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod p$

$$\text{Ex: } 3^{(5-1)} = 81 = 1 \pmod 5$$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots
Solve $x^2 = a \pmod p$ where p is a prime number.

1. $p \pmod 4$ can be either 1 or 3 – suppose it is 3

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

$$\text{Ex: } 3^{(5-1)} = 81 = 1 \pmod{5}$$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod{p}$;

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod{p}$; $a^{(4t+3-1)/2} = 1 \pmod{p}$;

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots
Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod{p}$; $a^{(4t+3-1)/2} = 1 \pmod{p}$; $a^{2t+1} = 1 \pmod{p}$

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod{p}$; $a^{(4t+3-1)/2} = 1 \pmod{p}$; $a^{2t+1} = 1 \pmod{p}$
 $a^{2t+2} = a \pmod{p}$;

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod p$

Ex: $3^{(5-1)} = 81 = 1 \pmod 5$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod p$ where p is a prime number.

1. $p \pmod 4$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod p$; $a^{(4t+3-1)/2} = 1 \pmod p$; $a^{2t+1} = 1 \pmod p$
 $a^{2t+2} = a \pmod p$; $a^{2(t+1)} = a \pmod p$;

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod p$

Ex: $3^{(5-1)} = 81 = 1 \pmod 5$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod p$ where p is a prime number.

1. $p \pmod 4$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod p$; $a^{(4t+3-1)/2} = 1 \pmod p$; $a^{2t+1} = 1 \pmod p$
 $a^{2t+2} = a \pmod p$; $a^{2(t+1)} = a \pmod p$; $(a^{t+1})^2 = a \pmod p$

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

Ex: $3^{(5-1)} = 81 = 1 \pmod{5}$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots

Solve $x^2 = a \pmod{p}$ where p is a prime number.

1. $p \pmod{4}$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod{p}$; $a^{(4t+3-1)/2} = 1 \pmod{p}$; $a^{2t+1} = 1 \pmod{p}$
 $a^{2t+2} = a \pmod{p}$; $a^{2(t+1)} = a \pmod{p}$; $(a^{t+1})^2 = a \pmod{p}$
4. so, if $p = 4t + 3$, then find the t , the square root of a is a^{t+1}

Mathematics of Cryptography

Modulo arithmetic – Fermat's Little Theorem

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod p$

Ex: $3^{(5-1)} = 81 = 1 \pmod 5$

$$36^{(29-1)} = 37711171281396032013366321198900157303750656 \\ = 1 \pmod{29}$$

Every number a has either 2 square roots $(\sqrt{a}, -\sqrt{a})$ or 0 square roots
Solve $x^2 = a \pmod p$ where p is a prime number.

1. $p \pmod 4$ can be either 1 or 3 – suppose it is 3
2. then $p = 4t + 3$ where t is some positive integer
3. but $a^{(p-1)/2} = 1 \pmod p$; $a^{(4t+3-1)/2} = 1 \pmod p$; $a^{2t+1} = 1 \pmod p$
 $a^{2t+2} = a \pmod p$; $a^{2(t+1)} = a \pmod p$; $(a^{t+1})^2 = a \pmod p$
4. so, if $p = 4t + 3$, then find the t , the square root of a is a^{t+1}
example: $p=19 = 4*4+3$, so $t=4$. Suppose a is 7
 $\sqrt{7} \pmod{19} = 7^5 \pmod{19} = 11 \pmod{19}$
check: $121 \pmod{19} = 7 \pmod{19}$

Mathematics of Cryptography

Finding a prime

Probability that a random number p is prime: $1/\ln(p)$

For 100 digit number this is $1/230$.

Mathematics of Cryptography

Finding a prime

Probability that a random number p is prime: $1/\ln(p)$

For 100 digit number this is $1/230$.

But how to test for being prime?

Mathematics of Cryptography

Finding a prime

Probability that a random number p is prime: $1/\ln(p)$

For 100 digit number this is $1/230$.

But how to test for being prime?

If p is prime and $0 < a < p$, then $a^{p-1} = 1 \pmod{p}$

$Pr(p \text{ isn't prime but } a^{p-1} = 1 \pmod{p})$ is small

Mathematics of Cryptography

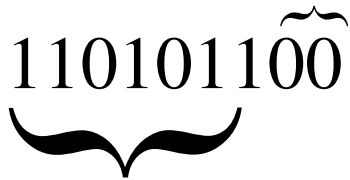
Finding a prime

Can always express a number $p-1$ as $2^b c$ for some odd number c .

ex: $48 = 2^4 3$

Here is the 2^b

110101100



Here is the odd number

Mathematics of Cryptography

Finding a prime

Can always express a number $p-1$ as $2^b c$ for some odd number c .

Then can compute $a^{p-1} \bmod p$ by computing $a^c \bmod p$ and squaring the result b times. If the result is not 1 then p is not prime.

Mathematics of Cryptography

Finding a prime

Trivial square roots of $1 \pmod{p}$: $1 \pmod{p}$ and $-1 \pmod{p}$

If p is prime, there are no nontrivial square roots of $1 \pmod{p}$

Let x be a square root of $1 \pmod{p}$. Then $x^2 = 1 \pmod{p}$.

Or, $(x-1)(x+1) = 0 \pmod{p}$.

But $x-1$ and $x+1$ are divisible by prime p . Hence, the product cannot be divisible by p . Therefore x does not exist.

Mathematics of Cryptography

Finding a prime

Consider $p-1 = 2^b c$ again. If p is prime then $a^c = 1 \pmod p$ or for some $r < b$, $a^{2^r c} = -1 \pmod p$.

Mathematics of Cryptography

Finding a prime

Choose a random odd integer p to test.

Calculate $b = \#$ times 2 divides $p-1$.

Calculate m such that $p = 1 + 2^b m$.

Choose a random integer a such that $0 < a < p$.

If $a^m \equiv 1 \pmod{p}$ || $a^{2^j m} \equiv -1 \pmod{p}$, for some $0 \leq j \leq b-1$, then p passes the test. A prime will pass the test for all a .

Mathematics of Cryptography

Finding a prime

Choose a random odd integer p to test.

Calculate $b = \#$ times 2 divides $p-1$.

Calculate m such that $p = 1 + 2^b m$.

Choose a random integer a such that $0 < a < p$.

If $a^m \equiv 1 \pmod{p}$ || $a^{2^j m} \equiv -1 \pmod{p}$, for some $0 \leq j \leq b-1$, then p passes the test. A prime will pass the test for all a .

A non prime number passes the test for at most 1/4 of all possible a .

So, repeat N times and probability of error is $(1/4)^N$.

Look at the applet

Mathematics of Cryptography

Finding a prime – importance to RSA

Choose e first, then find p and q so $(p-1)$ and $(q-1)$ are relatively prime to e

RSA is no less secure if e is always the same and small

Popular values for e are 3 and 65537

For $e = 3$, though, must pad message or else ciphertext = plaintext

Choose $p \equiv 2 \pmod{3}$ so $p-1 = 1 \pmod{3}$ so p is relatively prime to e

So, choose random odd number, multiply by 3 and add 2, then test for primality

Mathematics of Cryptography

Number Theory

Modular Arithmetic:

Two numbers **equivalent** mod n if their difference is multiple of n

example: 7 and 10 are equivalent mod 3 but not mod 4

$$7 \bmod 3 \equiv 10 \bmod 3 = 1; 7 \bmod 4 = 3, 10 \bmod 4 = 2.$$

Greatest Common Divisor:

Largest integer that evenly divides two given numbers

$$\gcd(3, 7) = 1; \gcd(294, 385) = 7;$$

$$294 = 42 \times 7; 385 = 55 \times 7;$$

Mathematics of Cryptography

Number Theory

Modular Arithmetic:

Two numbers **equivalent** mod n if their difference is multiple of n

example: 7 and 10 are equivalent mod 3 but not mod 4

$$7 \bmod 3 \equiv 10 \bmod 3 = 1; 7 \bmod 4 = 3, 10 \bmod 4 = 2.$$

Greatest Common Divisor:

Largest integer that evenly divides two given numbers

$$\gcd(3, 7) = 1; \gcd(294, 385) = 7;$$

$$294 = 42 \times 7; 385 = 55 \times 7;$$

Given integers m, n , suppose integer r is the smallest for which there exist integers u, v such that $r > 0$ and

$$u \times m + v \times n = r$$

then r is the greatest common divisor of m and n .

Mathematics of Cryptography

Number Theory

Modular Arithmetic:

Two numbers **equivalent** mod n if their difference is multiple of n

example: 7 and 10 are equivalent mod 3 but not mod 4

$$7 \bmod 3 \equiv 10 \bmod 3 = 1; 7 \bmod 4 = 3, 10 \bmod 4 = 2.$$

Greatest Common Divisor:

Largest integer that evenly divides two given numbers

$$\gcd(3, 7) = 1; \gcd(294, 385) = 7;$$

$$294 = 42 \times 7; 385 = 55 \times 7;$$

Given integers m, n , suppose integer r is the smallest for which there exist integers u, v such that $r > 0$ and

$$u \times m + v \times n = r$$

then r is the greatest common divisor of m and n .

If $p > r$ is common divisor then $u \times m/p + v \times n/p = \text{an integer} = r/p < 1$

Greatest Common Divisor

385

294

Greatest Common Divisor

$$\frac{385}{294} = 1 \text{ R } 91 \quad 91 = 1 \times 385 - 1 \times 294$$

Greatest Common Divisor

$$\frac{385}{294} = 1 \text{ R } 91 \quad \text{In other words we need the gcd of } 91 + 294 \text{ and } 294$$

Greatest Common Divisor

$\frac{385}{294} = 1 \text{ R } 91$ In other words we need the gcd of $91 + 294$ and 294
But this is the same gcd as for 91 and 294 !
because $(91+294)/a - 294/a = 91/a$
which must be an integer.

Greatest Common Divisor

385

294

$$91 = 1 \times 385 - 1 \times 294$$

294

91

Greatest Common Divisor

385

294

$$91 = 1 \times 385 - 1 \times 294$$

$$\frac{294}{91} = 3 \text{ R } 21 \quad 21 = 294 - 3(385 - 294) = -3 \times 385 + 4 \times 294$$

Greatest Common Divisor

385

294

$$91 = 1 \times 385 - 1 \times 294$$

294

91

$$21 = -3 \times 385 + 4 \times 294$$

91

21

Greatest Common Divisor

385

294

$$91 = 1 \times 385 - 1 \times 294$$

294

91

$$21 = -3 \times 385 + 4 \times 294$$

$$\frac{91}{21} = 4 \text{ R } 7 \quad 7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294$$

Greatest Common Divisor

385

294

294

91

91

21

$$7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294$$

21

7

Greatest Common Divisor

385

294

294

91

91

21

$$7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294$$

$$\frac{21}{7} = 3 \text{ R } 0$$

Greatest Common Divisor

385

294

294

91

91

21

$$7 = 1 \times 385 - 1 \times 294 - 4(-3 \times 385 + 4 \times 294) = 13 \times 385 - 17 \times 294$$

21

7

So, the gcd of 385 and 294 is 7

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m,n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of 89 mod 42:

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of 89 mod 42:

$$89 - 2 \times 42 = 5$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of 89 mod 42:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of $89 \bmod 42$:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

$$42 - 8 \times 5 = 2$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of $89 \bmod 42$:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

$$42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of $89 \bmod 42$:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

$$42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42$$

$$5 - 2 \times 2 = 1$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m,n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of $89 \bmod 42$:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

$$42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42$$

$$5 - 2 \times 2 \rightarrow 1 = 1 \times 89 - 2 \times 42 - 2(-8 \times 89 + 17 \times 42) = 17 \times 89 - 36 \times 42$$

Mathematics of Cryptography

Finding Multiplicative Inverses

Find an inverse of $m \bmod n$. That is, a number u such that $u \times m = 1 \bmod n$.

In other words, find u such that $u \times m + v \times n = 1$ for some v .

Apply previous algorithm ($\gcd(m, n)$) to get u, v but only if m and n are relatively prime.

Example:

Inverse of $89 \bmod 42$:

$$89 - 2 \times 42 \rightarrow 5 = 1 \times 89 - 2 \times 42$$

$$42 - 8 \times 5 \rightarrow 2 = 1 \times 42 - 8(1 \times 89 - 2 \times 42) = -8 \times 89 + 17 \times 42$$

$$5 - 2 \times 2 \rightarrow 1 = 1 \times 89 - 2 \times 42 - 2(-8 \times 89 + 17 \times 42) = 17 \times 89 - 36 \times 42$$

Conclusion: 17 is the inverse of $89 \bmod 42$! **Look at the applet**

Mathematics of Cryptography

Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

Mathematics of Cryptography

Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

Application: An army general about 2000 years ago sent by messenger a note to the emperor telling how many troops he had. But the number was encrypted in the following way:

dividing 602 by 3 gives a remainder of 2

dividing 602 by 5 gives a remainder of 2

dividing 602 by 7 gives a remainder of 0

dividing 602 by 11 gives a remainder of 8

So the message is: 2,2,0,8

It turns out that by the Chinese Remainder Theorem (CRT) it is possible to uniquely determine the number of troops provided all the divisions were by relatively prime numbers.

Mathematics of Cryptography

Chinese Remainder Theorem

There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

Application:

An old Chinese woman on the way to the market came upon a horse and rider. The horse stepped on her basket and crushed the eggs in her basket. The rider offered to pay for the broken eggs and asked how many eggs were in the basket. She did not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?

Mathematics of Cryptography

Chinese Remainder Theorem

If the prime factorization of n is $n_1 \times n_2 \times \dots \times n_k$ then the system of equations:

$$x \bmod n_1 = a_1 \qquad x = a_1 \bmod n_1$$

$$x \bmod n_2 = a_2 \qquad x = a_2 \bmod n_2$$

$$x \bmod n_3 = a_3 \qquad x = a_3 \bmod n_3$$

...

...

$$x \bmod n_k = a_k \qquad x = a_k \bmod n_k$$

has a unique solution x given any a_1, a_2, \dots, a_k where $x < n$.

Mathematics of Cryptography

Chinese Remainder Theorem

Why?

Define $\underline{n}^i = n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k$

This means, for each $1 \leq i \leq k$, there is an r_i and s_i such that

$$r_i n_i + s_i \underline{n}^i = 1$$

and r_i and s_i can be found using the gcd algorithm.

Since \underline{n}^i contains all n_j as factors except for n_i it is evenly divisible by all but n_i .

Then $s_i \underline{n}^i = 0 \pmod{n_j}$ for all $i \neq j$ and

$$s_i \underline{n}^i = 1 \pmod{n_i}$$

Mathematics of Cryptography

Chinese Remainder Theorem

Why?

The solution is

$$x = \sum_{i=1}^k a_i s_i \underline{n^i} \pmod{n_1 n_2 \dots n_k}$$

Therefore, as a check

$$x \pmod{n_1} = a_1 \times 1 + a_2 \times 0 + a_3 \times 0 + \dots + a_k \times 0 = a_1$$

$$x \pmod{n_2} = a_1 \times 0 + a_2 \times 1 + a_3 \times 0 + \dots + a_k \times 0 = a_2$$

$$x \pmod{n_3} = a_1 \times 0 + a_2 \times 0 + a_3 \times 1 + \dots + a_k \times 0 = a_3$$

...

$$x \pmod{n_k} = a_1 \times 0 + a_2 \times 0 + a_3 \times 0 + \dots + a_k \times 1 = a_k$$

Mathematics of Cryptography

Chinese Remainder Theorem

$$x \bmod n_1 = a_1 \qquad x \equiv a_1 \pmod{n_1}$$

$$x \bmod n_2 = a_2 \qquad x \equiv a_2 \pmod{n_2}$$

$$x \bmod n_3 = a_3 \qquad x \equiv a_3 \pmod{n_3}$$

...

...

$$x \bmod n_k = a_k \qquad x \equiv a_k \pmod{n_k}$$

has a unique solution x given any a_1, a_2, \dots, a_k where $x < n_1 n_2 \dots n_k$

Mathematics of Cryptography

Chinese Remainder Theorem

$$x \bmod n_1 = a_1 \qquad x \equiv a_1 \pmod{n_1}$$

$$x \bmod n_2 = a_2 \qquad x \equiv a_2 \pmod{n_2}$$

$$x \bmod n_3 = a_3 \qquad x \equiv a_3 \pmod{n_3}$$

...

...

$$x \bmod n_k = a_k \qquad x \equiv a_k \pmod{n_k}$$

Return to the original problem:

divide x by 3 and get a remainder of 2 $a_1 = 2$ $n_1 = 3$

divide x by 5 and get a remainder of 3 $a_2 = 3$ $n_2 = 5$

divide x by 7 and get a remainder of 2 $a_3 = 2$ $n_3 = 7$

What is the value of x that is no greater than $3 \times 5 \times 7$?

Mathematics of Cryptography

Chinese Remainder Theorem

$$x \bmod n_1 = a_1 \qquad x \equiv a_1 \pmod{n_1}$$

$$x \bmod n_2 = a_2 \qquad x \equiv a_2 \pmod{n_2}$$

$$x \bmod n_3 = a_3 \qquad x \equiv a_3 \pmod{n_3}$$

...

$$x \bmod n_k = a_k \qquad x \equiv a_k \pmod{n_k}$$

Return to the original problem:

divide x by 3 and get a remainder of 2 $a_1 = 2$ $n_1 = 3$

divide x by 5 and get a remainder of 3 $a_2 = 3$ $n_2 = 5$

divide x by 7 and get a remainder of 2 $a_3 = 2$ $n_3 = 7$

What is the value of x that is no greater than $3 \times 5 \times 7$?

Inverses of: $5 \times 7 \bmod 3 = 2$ $3 \times 7 \bmod 5 = 1$ $3 \times 5 \bmod 7 = 1$

Mathematics of Cryptography

Chinese Remainder Theorem

$$x \bmod n_1 = a_1 \qquad x \equiv a_1 \pmod{n_1}$$

$$x \bmod n_2 = a_2 \qquad x \equiv a_2 \pmod{n_2}$$

$$x \bmod n_3 = a_3 \qquad x \equiv a_3 \pmod{n_3}$$

...

...

$$x \bmod n_k = a_k \qquad x \equiv a_k \pmod{n_k}$$

Return to the original problem:

divide x by 3 and get a remainder of 2 $a_1 = 2$ $n_1 = 3$

divide x by 5 and get a remainder of 3 $a_2 = 3$ $n_2 = 5$

divide x by 7 and get a remainder of 2 $a_3 = 2$ $n_3 = 7$

What is the value of x that is no greater than $3 \times 5 \times 7$?

Inverses of: $5 \times 7 \bmod 3 = 2$ $3 \times 7 \bmod 5 = 1$ $3 \times 5 \bmod 7 = 1$

$$x = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{3 \times 5 \times 7} = 23 \text{ (128, 233, ...)}$$

Mathematics of Cryptography

Chinese Remainder Theorem

Second problem:

$$x = 1 \pmod{2} \rightarrow x = 2 \times t + 1$$

$$x = 1 \pmod{3} \rightarrow x = 3 \times p + 1$$

$$x = 1 \pmod{4} \rightarrow x = 4 \times r + 1$$

$$x = 1 \pmod{5} \rightarrow x = 5 \times s + 1$$

$$x = 1 \pmod{6} \rightarrow x = 6 \times q + 1$$

$$x = 0 \pmod{7} \rightarrow x = 7 \times w$$

Mathematics of Cryptography

Chinese Remainder Theorem

Second problem: Whoops! not a prime factorization

$$x = 1 \pmod{2} \rightarrow x = 2 \times t + 1$$

$$x = 1 \pmod{3} \rightarrow x = 3 \times p + 1$$

$$x = 1 \pmod{4} \rightarrow x = 4 \times r + 1$$

$$x = 1 \pmod{5} \rightarrow x = 5 \times s + 1$$

$$x = 1 \pmod{6} \rightarrow x = 6 \times q + 1$$

$$x = 0 \pmod{7} \rightarrow x = 7 \times w$$

$$\text{so, } 2 \times t = 3 \times p = 4 \times r = 5 \times s = 6 \times q$$

$$\text{from last two } q = v \times 5 \text{ and } s = v \times 6$$

$$\text{but } r = 3 \times q / 2 \text{ so } q = v \times 2 \times 5 \text{ and } s = v \times 2 \times 6 \text{ making } r = v \times 3 \times 5$$

$$\text{also } p = 2 \times q = v \times 4 \times 5$$

$$\text{and } t = 2 \times r = v \times 30$$

$$\text{so } x = 60 \times v + 1; n = 7 \times w$$

$$7 \times w = 60 \times v + 1$$

Mathematics of Cryptography

Chinese Remainder Theorem

Immediate consequence:

Suppose everyone's RSA public key e part is 3. Consider the same message sent to three people. These are:

$$c[1] = m^3 \bmod n[1]$$

$$c[2] = m^3 \bmod n[2]$$

$$c[3] = m^3 \bmod n[3]$$

By the Chinese Remainder Theorem

One can compute $m^3 \bmod n[1] \times n[2] \times n[3]$

Since m is smaller than any of the $n[i]$, m^3 is known and taking the cube root finds m .

Mathematics of Cryptography

Z^*_n

All numbers less than n that are relatively prime with n

Examples: $Z^*_{10} = \{ 1, 3, 7, 9 \}$; $Z^*_{15} = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

If numbers a, b are members of Z^*_n then so is $a \times b \bmod n$.

Examples: $4 \times 11 \bmod 15 = 44 \bmod 15 = 14$;

$13 \times 14 \bmod 15 = 182 \bmod 15 = 2$.

Mathematics of Cryptography

Z^*_n

All numbers less than n that are relatively prime with n

Examples: $Z^*_{10} = \{ 1, 3, 7, 9 \}$; $Z^*_{15} = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

If numbers a, b are members of Z^*_n then so is $a \times b \bmod n$.

Examples: $4 \times 11 \bmod 15 = 44 \bmod 15 = 14$;

$13 \times 14 \bmod 15 = 182 \bmod 15 = 2$.

Why?

Since a and b are relatively prime to n there must be integers s.t.

$u \times a + v \times n = 1$ and $w \times b + x \times n = 1$.

Mathematics of Cryptography

Z^*_n

All numbers less than n that are relatively prime with n

Examples: $Z^*_{10} = \{ 1, 3, 7, 9 \}$; $Z^*_{15} = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

If numbers a, b are members of Z^*_n then so is $a \times b \pmod n$.

Examples: $4 \times 11 \pmod{15} = 44 \pmod{15} = 14$;

$13 \times 14 \pmod{15} = 182 \pmod{15} = 2$.

Why?

Since a and b are relatively prime to n there must be integers s.t.

$u \times a + v \times n = 1$ and $w \times b + x \times n = 1$.

Multiply both equations:

$$(u \times w) \times a \times b + (u \times x \times a + v \times w \times b + x \times v \times n) \times n = 1$$

Hence $a \times b$ is relatively prime to n .

Mathematics of Cryptography

Euler's Totient Function:

Defined: $\phi(n)$ is number of elements in Z^*_n .

Example: $\phi(7) = 6$ ($\{1,2,3,4,5,6\}$) ; $\phi(10) = 4$ ($\{1,3,7,9\}$)

Suppose $n = p \times q$ and p and q are relatively prime

Example: $\phi(70)$:

$\{ 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47,$
 $51, 53, 57, 59, 61, 67, 69 \}$

$$\phi(70) = \phi(7)\phi(10) = 24.$$

Why?

Mathematics of Cryptography

Euler's Totient Function:

Defined: $\phi(n)$ is number of elements in Z^*_n .

Example: $\phi(7) = 6$ ($\{1,2,3,4,5,6\}$) ; $\phi(10) = 4$ ($\{1,3,7,9\}$)

Suppose $n = p \times q$ and p and q are relatively prime

Example: $\phi(70)$:

$\{ 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69 \}$

$$\phi(70) = \phi(7)\phi(10) = 24.$$

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number m and

$$\begin{array}{lll} m_p = m \bmod p & 1 = 29 \bmod 7 & 4 = 39 \bmod 7 \\ m_q = m \bmod q & 9 = 29 \bmod 10 & 9 = 39 \bmod 10 \end{array}$$

Mathematics of Cryptography

Euler's Totient Function:

Defined: $\phi(n)$ is number of elements in Z^*_n .

Example: $\phi(7) = 6$ ($\{1,2,3,4,5,6\}$) ; $\phi(10) = 4$ ($\{1,3,7,9\}$)

Suppose $n = p \times q$ and p and q are relatively prime

Example: $\phi(70)$:

$\{ 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 51, 53, 57, 59, 61, 67, 69 \}$

$$\phi(70) = \phi(7)\phi(10) = 24.$$

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number m and

$$m_p = m \bmod p$$

$$m_q = m \bmod q$$

If m is relatively prime to pq , then there are integers u, v , such that $um + vpq = 1$.

Mathematics of Cryptography

Euler's Totient Function:

Substituting $m = m_p + kp$ gives

$$um_p + (uk + vq)p = 1$$

so m_p is relatively prime to p . Same for m_q and q .

Therefore, m in Z^*_{pq} means m_p is in Z^*_p and m_q is in Z^*_q .

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number m and

$$m_p = m \bmod p$$

$$m_q = m \bmod q$$

If m is relatively prime to pq , then there are integers u, v , such that $um + vpq = 1$.

Mathematics of Cryptography

Euler's Totient Function:

Substituting $m = m_p + kp$ gives

$$um_p + (uk + vq)p = 1$$

so m_p is relatively prime to p . Same for m_q and q .

Therefore, m in Z^*_{pq} means m_p is in Z^*_p and m_q is in Z^*_q .

Similar tricks can be used to show that m_q in Z^*_q and m_p in Z^*_p imply m in Z^*_{pq} .

Why? By the Chinese Remainder Theorem there is a 1-1 correspondence between a number m and

$$m_p = m \bmod p$$

$$m_q = m \bmod q$$

If m is relatively prime to pq , then there are integers u, v , such that $um + vpq = 1$.

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , $a^{\phi(n)} = 1 \pmod n$.

Why?

By example: suppose $n = 10$, $a = 3$. Multiply all elements of $Z^*_n = \{ 1, 3, 7, 9 \}$ to get $x = 189$. But $x \pmod{10} = 9$ which is an element of Z^*_n . The inverse of x is 9.

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*n , $a^{\phi(n)} = 1 \pmod n$.

Why?

By example: suppose $n = 10$, $a = 3$. Multiply all elements of $Z^*n = \{ 1, 3, 7, 9 \}$ to get $x = 189$. But $x \pmod{10} = 9$ which is an element of Z^*n . The inverse of x is 9.

Multiply all elements of Z^*n by 3 and multiply all those numbers:

$$(3 \times 1) \times (3 \times 3) \times (3 \times 7) \times (3 \times 9) = 3^{\phi(n)} \times x$$

But $3 \times 1 = 3$, $3 \times 3 = 9$, $3 \times 7 = 1$, $3 \times 9 = 7$ (all mod 10)

Hence $a^{\phi(n)} \times x = x \pmod n$.

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

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Why?

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Why? $a^{(k \times \phi(n) + 1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Why? $a^{(k \times \phi(n) + 1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all a and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$,
if $n = p \times q$, p and q are prime then $\phi(n) = (p-1) \times (q-1)$

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Why? $a^{(k \times \phi(n) + 1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all a and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$,
if $n = p \times q$, p and q are prime then $\phi(n) = (p-1) \times (q-1)$

Why?

Mathematics of Cryptography

Euler's Theorem:

For all a in Z^*_n , and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Why? $a^{(k \times \phi(n) + 1)} = (a^{\phi(n)})^k \times a = 1^k \times a = a$

For all a and any non-neg int k , $a^{(k \times \phi(n) + 1)} = a \pmod n$,
if $n = p \times q$, p and q are prime then $\phi(n) = (p-1) \times (q-1)$

Why? Only interesting case: a is a multiple of p or q .

Suppose a is a multiple of q .

Since a is relatively prime to p , $a^{\phi(p)} = 1 \pmod p$.

Since $\phi(n) = \phi(p) \times \phi(q)$, $(\pmod p)$

$a^{(k \times \phi(n) + 1)} = (a^{(\phi(p) \times \phi(q))})^k \times a = 1^{(k \times \phi(n))} \times a = a \pmod p$ and

$a = 0 \pmod q$ so $a^{(k \times \phi(n) + 1)} = 0 = a \pmod q$.

By CRT $a^{(k \times \phi(n) + 1)} = a \pmod n$.

Mathematics of Cryptography

RSA:

$$n = p * q$$

$$\phi(n) = (p-1) * (q-1)$$

e – relatively prime to $\phi(n)$

d – such that $e * d - 1$ divisible by $\phi(n)$

hence $(e * d - 1) / \phi(n) = k$, a positive integer

$$\text{so } e * d = k * \phi(n) + 1$$

$$\text{therefore } m^{e * d} = m^{k * \phi(n) + 1} = m \pmod n$$