An Application of Number Theory, the RSA Cryptosystem

Ngày 10 tháng 12 năm 2010

Securing Transactions

Question

Mr. Nguyen sells expensive jewelry. He has an interesting idea for a business model. Each customer will have access to boxes with a combination lock. Once a person grabs a box he can set his own private combination lock. An open box can be closed by anyone, but only the owner knows the combination and can open it. The content of any open box sent between persons will be stolen.

You wish to buy an expensive gift for your significant other's birthday. This means money will have to be sent to Mr. Nguyen (who is honest and trustworthy) and the gift delivered to you. Transaction details, such as item, price etc. can be discussed by phone.

Question

Mr. Nguyen sells expensive jewelry. He has an interesting idea for a business model. Each customer will have access to boxes with a combination lock. Once a person grabs a box he can set his own private combination lock. An open box can be closed by anyone, but only the owner knows the combination and can open it. The content of any open box sent between persons will be stolen.

You wish to buy an expensive gift for your significant other's birthday. This means money will have to be sent to Mr. Nguyen (who is honest and trustworthy) and the gift delivered to you. Transaction details, such as item, price etc. can be discussed by phone.

Securing Transactions

Question

Mr. Nguyen sells expensive jewelry. He has an interesting idea for a business model. Each customer will have access to boxes with a combination lock. Once a person grabs a box he can set his own private combination lock. An open box can be closed by anyone, but only the owner knows the combination and can open it. The content of any open box sent between persons will be stolen.
You wish to buy an expensive gift for your significant other's birthday. This means money will have to be sent to Mr. Nguyen (who is honest and trustworthy) and the gift delivered to you. Transaction details, such as item, price etc. can be discussed by phone.

How can we accomplish this?

Discussion

This is exactly how business transactions are being conducted on the internet today, except that the boxes are virtual boxes. Closing a box is accomplished by encrypting the message. So while the message is traveling on the internet, being exposed to hackers and others, it is encrypted using a “key”. Only the owner of the key knows how to open the box and retrieve its content.

Discussion

This is exactly how business transactions are being conducted on the internet today, except that the boxes are virtual boxes. Closing a box is accomplished by encrypting the message. So while the message is traveling on the internet, being exposed to hackers and others, it is encrypted using a "key". Only the owner of the key knows how to open the box and retrieve its content.

Question

The question faced scientists was how to design a system with the following properties:

Discussion

This is exactly how business transactions are being conducted on the internet today, except that the boxes are virtual boxes. Closing a box is accomplished by encrypting the message. So while the message is traveling on the internet, being exposed to hackers and others, it is encrypted using a "key". Only the owner of the key knows how to open the box and retrieve its content.

Question

The question faced scientists was how to design a system with the following properties:

1. *A group of particpants can securely communicate with each other over an open system.*

Discussion

This is exactly how business transactions are being conducted on the internet today, except that the boxes are virtual boxes. Closing a box is accomplished by encrypting the message. So while the message is traveling on the internet, being exposed to hackers and others, it is encrypted using a "key". Only the owner of the key knows how to open the box and retrieve its content.

Question

The question faced scientists was how to design a system with the following properties:

1. *A group of particpants can securely communicate with each other over an open system.*
2. *How can anyone send a message to bob so no one except Bob will be able to understand the message.*

Discussion

This is exactly how business transactions are being conducted on the internet today, except that the boxes are virtual boxes. Closing a box is accomplished by encrypting the message. So while the message is traveling on the internet, being exposed to hackers and others, it is encrypted using a "key". Only the owner of the key knows how to open the box and retrieve its content.

Question

The question faced scientists was how to design a system with the following properties:

1. *A group of particpants can securely communicate with each other over an open system.*
2. *How can anyone send a message to bob so no one except Bob will be able to understand the message.*
3. *Can messages be "signed'?.*

Discussion

Until the mid-70's encryptions were done using private keys. Two persons or institutions that needed to establish secure communications shared a private key they used for encryption.

The system worked quite well, except for one problem: how to share keys.

DES, (Data Encryption Standard) was a popular private key system that was widely used by many governments and institutions.

It was recently replaced by another system, AES (Advanced Encryption Standard).

Discussion

Until the mid-70's encryptions were done using private keys. Two persons or institutions that needed to establish secure communications shared a private key they used for encryption.

The system worked quite well, except for one problem: how to share keys.

DES, (Data Encryption Standard) was a popular private key system that was widely used by many governments and institutions.

It was recently replaced by another system, AES (Advanced Encryption Standard).

RSA Public Key System

Discussion

Until the mid-70's encryptions were done using private keys. Two persons or institutions that needed to establish secure communications shared a private key they used for encryption.

The system worked quite well, except for one problem: how to share keys.

DES, (Data Encryption Standard) was a popular private key system that was widely used by many governments and institutions.

It was recently replaced by another system, AES (Advanced Encryption Standard).

In 1976 Rivest, Shamir and Adelman proposed the public key cryptosystem: RSA.

Each key consisted of two parts, a public part used for encryption and a private part used for decryption.

1. Every message can be coded as an integer M.

RSA

Each key consisted of two parts, a public part used for encryption and a private part used for decryption.

1. Every message can be coded as an integer M.
2. Public key: (K, e) where $K = pq,\ p, q$ prime numbers, $gcd(e, (p-1)(q-1)) = 1$.

RSA

Each key consisted of two parts, a public part used for encryption and a private part used for decryption.

1. Every message can be coded as an integer M.
2. Public key: (K, e) where $K = pq,\ p, q$ prime numbers, $gcd(e, (p-1)(q-1)) = 1$.
3. To encrypt the message M, coded as an integer, we calculate $EM = M^e \bmod K$ and send EM to the owner of the public key (K, e).

Each key consisted of two parts, a public part used for encryption and a private part used for decryption.

1. Every message can be coded as an integer M.
2. Public key: (K, e) where $K = pq,\ p, q$ prime numbers, $gcd(e, (p-1)(q-1)) = 1$.
3. To encrypt the message M, coded as an integer, we calculate $EM = M^e \bmod K$ and send EM to the owner of the public key (K, e).
4. Decryption: The key owner first finds $d = e^{-1} \bmod (p-1)(q-1)$.

RSA

Each key consisted of two parts, a public part used for encryption and a private part used for decryption.

1. Every message can be coded as an integer M.
2. Public key: (K, e) where $K = pq,\ p, q$ prime numbers, $gcd(e, (p-1)(q-1)) = 1$.
3. To encrypt the message M, coded as an integer, we calculate $EM = M^e \bmod K$ and send EM to the owner of the public key (K, e).
4. Decryption: The key owner first finds $d = e^{-1} \bmod (p-1)(q-1)$.
5. To retrieve M, the owner of the key (K, e) calculates: $EM^d \bmod K = M$.

Prime numbers, key facts

The following theorems play a central role discussing primes and factorization.

1. T1: $GF(p) = \{0, 1, \ldots, p-1\}$ is a field (addition and multiplication are done mod p)

Prime numbers, key facts

The following theorems play a central role discussing primes and factorization.

1. T1: $GF(p) = \{0, 1, \ldots, p-1\}$ is a field (addition and multiplication are done mod p)
2. T2: $GF(p)$ has primitve elements. $\alpha \in GF(p)$ is **primitive** if $\{\alpha^i |\ i = 0, 1, \ldots p-2\} = \{0, 1, 2, \ldots, p-1\}$.

Prime numbers, key facts

The following theorems play a central role discussing primes and factorization.

1. T1: $GF(p) = \{0, 1, \ldots, p-1\}$ is a field (addition and multiplication are done mod p)
2. T2: $GF(p)$ has primitve elements. $\alpha \in GF(p)$ is **primitive** if $\{\alpha^i | \ i = 0, 1, \ldots p-2\} = \{0, 1, 2, \ldots, p-1\}$.
3. T3: If $p(x)$ is a polynomial with coefficients in $GF(p)$ and $f(\beta) = 0$ then $p(x) = (x - \beta)p_1(x)$ where $p_1(x)$ is a polynomial with coefficients in $GF(p)$.

Prime numbers, key facts

The following theorems play a central role discussing primes and factorization.

1. T1: $GF(p) = \{0, 1, \ldots, p-1\}$ is a field (addition and multiplication are done mod p)
2. T2: $GF(p)$ has primitve elements. $\alpha \in GF(p)$ is **primitive** if $\{\alpha^i | \; i = 0, 1, \ldots p-2\} = \{0, 1, 2, \ldots, p-1\}$.
3. T3: If $p(x)$ is a polynomial with coefficients in $GF(p)$ and $f(\beta) = 0$ then $p(x) = (x - \beta)p_1(x)$ where $p_1(x)$ is a polynomial with coefficients in $GF(p)$.
4. T4: A finite field has p^n (p prime) elements and is unique upto isomorphism.

Theorem (Fermat's theorem)

If p is prime and $a < p$ then $a^{p-1} \bmod p = 1$.

Theorem (Fermat's theorem)

If p is prime and $a < p$ then $a^{p-1} \bmod p = 1$.

Chứng minh.

Since $GF(p)$ is a field for any
$a \in GF(p) \quad \{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, \ldots, p-1\}$.
So $a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1)$
$a^{p-1} \cdot \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} i \bmod p \Rightarrow a^{p-1} = 1 \bmod p$ □

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2.
   - 11 *is prime, so* $7^{10} \bmod 11 = 1$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. • 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.
4. • $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.
4. - $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$
   $7^{341235} \bmod 31 = 7^{341220} 7^{15} \bmod 31 = 7^{15} \bmod 31.$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.
4. - $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$
   $7^{341235} \bmod 31 = 7^{341220} 7^{15} \bmod 31 = 7^{15} \bmod 31.$
   $7^2 \bmod 31 = 18, \;\; 7^3 \bmod 31 = 7 \cdot 18 \bmod 31 =$
   $126 \bmod 31 = 2$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$*.*
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
     $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$*.*
4. - $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$
     $7^{341235} \bmod 31 = 7^{341220} 7^{15} \bmod 31 = 7^{15} \bmod 31.$
     $7^2 \bmod 31 = 18, \quad 7^3 \bmod 31 = 7 \cdot 18 \bmod 31 =$
     $126 \bmod 31 = 2$
     $7^5 \bmod 31 = 7^3 \cdot 7^2 \bmod 31 = 1.$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$*.*
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
     $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$*.*
4. - $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$
     $7^{341235} \bmod 31 = 7^{341220} 7^{15} \bmod 31 = 7^{15} \bmod 31.$
     $7^2 \bmod 31 = 18, \;\; 7^3 \bmod 31 = 7 \cdot 18 \bmod 31 =$
     $126 \bmod 31 = 2$
     $7^5 \bmod 31 = 7^3 \cdot 7^2 \bmod 31 = 1.$
     So if $x = 7^{341235}$ *then we have:*
     $x \bmod 11 = 10, \;\; x \bmod 31 = 1.$

Fermat's theorem can be applied to simplify some intimidating looking computations:

Example

1. *Calculate* $7^{341235} \bmod 11$.
2. - 11 *is prime, so* $7^{10} \bmod 11 = 1$
   $7^{341235} \bmod 11 = (7^{10})^{34123} \cdot 7^5 \bmod 11 = 7^5 \bmod 11 = 10$
3. *Calculate* $7^{341235} \bmod 341$.
4. - $341 = 31 \cdot 11, \quad 7^{341235} \bmod 11 = 10.$
   $7^{341235} \bmod 31 = 7^{341220} 7^{15} \bmod 31 = 7^{15} \bmod 31.$
   $7^2 \bmod 31 = 18, \;\; 7^3 \bmod 31 = 7 \cdot 18 \bmod 31 =$
   $126 \bmod 31 = 2$
   $7^5 \bmod 31 = 7^3 \cdot 7^2 \bmod 31 = 1.$
   So if $x = 7^{341235}$ *then we have:*
   $x \bmod 11 = 10, \;\; x \bmod 31 = 1.$
   We can now use the Chinese Reaminder Theorem and get:
   $7^{341235} \bmod 341 = 32.$

Fermat's theorem can be used to test whether an integer is composite (not prime).

Fermat's theorem can be used to test whether an integer is composite (not prime).

Given an integer n, if $a^{n-1} \bmod n \neq 1, \; a < n$ then n is composite.

Fermat's theorem can be used to test whether an integer is composite (not prime).

Given an integer n, if $a^{n-1} \bmod n \neq 1, \; a < n$ then n is composite.

But what if $a^{n-1} = 1$?
For example: $2^{340} \bmod 341 = 1 \quad but \; 341 = 11 \cdot 31$
$a^{1728} \bmod 1729 = 1 \; \forall a$ relatively prime to 1729.

Question

Can you prove it? It is not difficult, give it a try.

Question (Challenge)

The other day we found the 163 *digits long key below on the internet. It is not prime, easy to check.*

$2^{Key-1} \bmod Key \neq 1$

Can we find its prime factors?

Key =
1193098423264097759646037965385887599016380476452
72854129917551358235578179312630945926936573377803
05097493118591879028040057842613777270672354255530
86083970158319

Question (Challenge)

The other day we found the 163 *digits long key below on the internet. It is not prime, easy to check.*

$2^{Key-1} \bmod Key \neq 1$

Can we find its prime factors?

Key =
1193098423264097759646037965385887599016380476452
72854129917551358235578179312630945926936573377803
05097493118591879028040057842613777270672354255530
86083970158319

Question

Are there any other ways to factor integers besides trying the GCD of the integer with smaller integers?

Is p really a prime number?

Question

Is there a way to certify that a given number p is indeed prime?

Is p really a prime number?

Question

Is there a way to certify that a given number p is indeed prime?

Theorem (Wallis)

p is prime if and only if $(p-1)! \bmod p = -1$.

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N - 1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N-1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N - 1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Answer: NOTHING. N can be composite, or prime.

Example

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N-1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Answer: NOTHING. N can be composite, or prime.

Example

1. $2^{340} \bmod 341 = 1$ *but* $341 = 11 \cdot 31$.

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N-1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Answer: NOTHING. N can be composite, or prime.

Example

1. $2^{340} \bmod 341 = 1$ *but* $341 = 11 \cdot 31$.
2. *But* $3^{340} \bmod 341 = 56$ *proves that* 341 *is composite.*

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N-1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Answer: NOTHING. N can be composite, or prime.

Example

1. $2^{340} \bmod 341 = 1$ *but* $341 = 11 \cdot 31$.
2. *But* $3^{340} \bmod 341 = 56$ *proves that* 341 *is composite.*
3. *On the other hand, if* $gcd(a, 1729) = 1$ *then* $a^{1728} mod 1729 = 1$.

Miller-Rabin Test

Let N be an integer. By Fermat's theorem if N is prime then $a^{N-1} \bmod N = 1$. This calculation can be executed very fast on integers with a few thousand digits. This means that if for some $1 < a < N-1,\ a^{N-1} \bmod N \neq 1$ then N is definitely not a prime number.

But what can we conclude if $a^{N-1} \bmod N = 1$?

Answer: NOTHING. N can be composite, or prime.

Example

1. $2^{340} \bmod 341 = 1$ *but* $341 = 11 \cdot 31$.
2. *But* $3^{340} \bmod 341 = 56$ *proves that* 341 *is composite.*
3. *On the other hand, if* $gcd(a, 1729) = 1$ *then* $a^{1728} mod 1729 = 1$.
4. *Since* $\phi(1729) = 1729(1 - \frac{1}{7})(1 - \frac{1}{13})(1 - \frac{1}{19}) = 1296$ *if we select a randomly we do not have a good chance to find an integer that will prove that* 1729 *is not a prime number .*

Miller-Rabin Test

Numbers N like 1729 for which $a^{N-1} \bmod N = 1 \ \forall a$ relatively prime to N are called *Carmichael numbers*. They are rare, but there are infinitely many of them.

Miller-Rabin Test

Numbers N like 1729 for which $a^{N-1} \bmod N = 1\ \forall a$ relatively prime to N are called *Carmichael numbers*. They are rare, but there are infinitely many of them.

So Fermat's theorem is not a good test for primality. We need a better test.

Theorem (Miller-Rabin Test)

Let N be an integer, $N - 1 = 2^m \cdot (2k + 1)$*.*

An integer n is **NOT** *a "composite-witness" for N if:*

In other words, the test fails to prove that N is composite.

Miller-Rabin Test

Numbers N like 1729 for which $a^{N-1} \bmod N = 1\ \forall a$ relatively prime to N are called *Carmichael numbers*. They are rare, but there are infinitely many of them.

So Fermat's theorem is not a good test for primality. We need a better test.

Theorem (Miller-Rabin Test)

Let N be an integer, $N - 1 = 2^m \cdot (2k+1)$.

An integer n is **NOT** *a "composite-witness" for N if:*

1. *For some* $1 \le i \le m, \quad n^{(2k+1)2^i} \bmod N = -1$.

In other words, the test fails to prove that N is composite.

Numbers N like 1729 for which $a^{N-1} \bmod N = 1\ \forall a$ relatively prime to N are called *Carmichael numbers*. They are rare, but there are infinitely many of them.

So Fermat's theorem is not a good test for primality. We need a better test.

Theorem (Miller-Rabin Test)

Let N be an integer, $N - 1 = 2^m \cdot (2k+1)$.

An integer n is **NOT** *a "composite-witness" for N if:*

1. *For some $1 \leq i \leq m$,* $\quad n^{(2k+1)2^i} \bmod N = -1$.
2. *Or $n^{(2k+1)2^i} \bmod N = 1$ and $n^{2k+1} \bmod N = 1$*

In other words, the test fails to prove that N is composite.

Miller-Rabin Test

Chứng minh.

If p is prime then by Fermat's theorem $a^{p-1} \bmod p = 1$.
So $a^{(p-1)/2} \bmod p = \sqrt{1} = \pm 1$.
If $a^{(p-1)/2} \bmod p = -1$ then the test stops. In other words, it will not say that p is composite.
If $a^{(p-1)/2} \bmod p = 1$ then we calculate $a^{(p-1)/4} \bmod p = \pm 1$
We continue until we reach $a^{2k+1} \bmod p$ □

We skip the important part of the proof. They proved that if N is composite then more than 50% of the integers $a < N$ will be composite-witnesses. In other words, to test whether an integer p is prime, we randomly select say 100 integers $a < p$ and apply to them the Miller-Rabin test. If the test fails, we assume that p is a prime number. The probabilty that we made a mistake, that is decided that p is prime while in fact it is not, is less then $\left(\frac{1}{2}\right)^{100}$.

Example

Example

1. 1729 *is a composite integer. Indeed* $1728 = 2^6 \cdot 3^3$ *and* $3^{1728/2^i} \bmod 1729 = 1$ *but* $3^{1728/64} \bmod 1729 = 664$ *proving that* 1729 *is composite.*

Example

1. *1729 is a composite integer. Indeed* $1728 = 2^6 \cdot 3^3$ *and* $3^{1728/2^i} \bmod 1729 = 1$ *but* $3^{1728/64} \bmod 1729 = 664$ *proving that* 1729 *is composite.*
2. $c = 9746347772161$ *is a Carmichael number.*

Example

1. 1729 *is a composite integer. Indeed* $1728 = 2^6 \cdot 3^3$ *and* $3^{1728/2^i} \bmod 1729 = 1$ *but* $3^{1728/64} \bmod 1729 = 664$ *proving that* 1729 *is composite.*
2. $c = 9746347772161$ *is a Carmichael number.*
3. $3^{9746347772160} \bmod 9746347772161 = 1$*.*

Example

1. *1729 is a composite integer. Indeed* $1728 = 2^6 \cdot 3^3$ *and* $3^{1728/2^i} \bmod 1729 = 1$ *but* $3^{1728/64} \bmod 1729 = 664$ *proving that* 1729 *is composite.*
2. $c = 9746347772161$ *is a Carmichael number.*
3. $3^{9746347772160} \bmod 9746347772161 = 1$*.*
4. $3^{9746347772160/2} \bmod 9746347772161 = 1$*, no decission. So we continue.*

Example

1. *1729 is a composite integer. Indeed* $1728 = 2^6 \cdot 3^3$ *and* $3^{1728/2^i} \bmod 1729 = 1$ *but* $3^{1728/64} \bmod 1729 = 664$ *proving that* 1729 *is composite.*
2. $c = 9746347772161$ *is a Carmichael number.*
3. $3^{9746347772160} \bmod 9746347772161 = 1$.
4. $3^{9746347772160/2} \bmod 9746347772161 = 1$, *no decission. So we continue.*
5. $3^{9746347772160/4} \bmod 9746347772161 = 4485448662696$ *proving that c is composite.*

Factoring

Discussion

Factoring

Discussion

1. *To implement RSA we need to manufacture large primes.*

Factoring

Discussion

1. *To implement RSA we need to manufacture large primes.*
2. *The Miller-Rabin test is commonly used for this purpose.*

Factoring

Discussion

1. *To implement RSA we need to manufacture large primes.*
2. *The Miller-Rabin test is commonly used for this purpose.*
3. *There are also efficient algorithms to manufacture "certified" primes.*

Factoring

Discussion

1. *To implement RSA we need to manufacture large primes.*
2. *The Miller-Rabin test is commonly used for this purpose.*
3. *There are also efficient algorithms to manufacture "certified" primes.*
4. *Are all large primes safe?*

Square roots

Most integers are not perfect squares. Finding the square root or identifying that it is not a perfect square is very easy. Yet in modular arithmetic the situation is drastically different.

Square roots

Most integers are not perfect squares. Finding the square root or identifying that it is not a perfect square is very easy. Yet in modular arithmetic the situation is drastically different.

Half the positive integres mod a prime number p are *quadratic residues*. While finding their square roots is not difficult it is a bit trickier than finding the square root of an integer.

Square roots

Most integers are not perfect squares. Finding the square root or identifying that it is not a perfect square is very easy. Yet in modular arithmetic the situation is drastically different.

Half the positive integres mod a prime number p are *quadratic residues*. While finding their square roots is not difficult it is a bit trickier than finding the square root of an integer.

Finding the square root of an integer mod $p \cdot q$ where p, q are primes is dramatically different. Actually it is as difficult as factoring. In other words, if there was a fast calculation of $\sqrt{n} \bmod p \cdot q$ then we would have a fast factorization.

Square roots

Most integers are not perfect squares. Finding the square root or identifying that it is not a perfect square is very easy. Yet in modular arithmetic the situation is drastically different.

Half the positive integres mod a prime number p are *quadratic residues*. While finding their square roots is not difficult it is a bit trickier than finding the square root of an integer.

Finding the square root of an integer mod $p \cdot q$ where p, q are primes is dramatically different. Actually it is as difficult as factoring. In other words, if there was a fast calculation of $\sqrt{n}$ mod $p \cdot q$ then we would have a fast factorization.

We shall start by learning how to find $\sqrt{n}$ mod p.

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.

$\sqrt{n} \mod p$

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.
2. n is a quadratic residue mod p if and only if $n = \alpha^{2k} \mod p$.

$\sqrt{n} \mod p$

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.
2. n is a quadratic residue mod p if and only if $n = \alpha^{2k} \mod p$.
3. n is a quadratic residue mod p if and only if $n^{\frac{p-1}{2}} \mod p = 1$.

$\sqrt{n} \mod p$

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.
2. n is a quadratic residue mod p if and only if $n = \alpha^{2k} \mod p$.
3. n is a quadratic residue mod p if and only if $n^{\frac{p-1}{2}} \mod p = 1$.
4. **Claim:** If n is a quadratice residue mod p then we can find an integer β such that $n^{2m+1}\beta^{2s} \mod p = 1$

$\sqrt{n} \mod p$

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.
2. n is a quadratic residue mod p if and only if $n = \alpha^{2k} \mod p$.
3. n is a quadratic residue mod p if and only if $n^{\frac{p-1}{2}} \mod p = 1$.
4. **Claim:** If n is a quadratice residue mod p then we can find an integer β such that $n^{2m+1}\beta^{2s} \mod p = 1$
5. $\sqrt{n} \mod p = n^{m+1}\beta^{s} \mod p$

$\sqrt{n} \mod p$

1. Recall: $GF(p)$ has primitve elements. Let α be a primitive element of $GF(p)$.
2. n is a quadratic residue mod p if and only if $n = \alpha^{2k} \mod p$.
3. n is a quadratic residue mod p if and only if $n^{\frac{p-1}{2}} \mod p = 1$.
4. **Claim:** If n is a quadratice residue mod p then we can find an integer β such that $n^{2m+1}\beta^{2s} \mod p = 1$
5. $\sqrt{n} \mod p = n^{m+1}\beta^{s} \mod p$
6. We will not have to find a primitive element.

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k + 1)$.

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k+1)$.
4. Note: $n^{\frac{p-1}{4}} \mod p = \pm 1$. Repeat calculating $n^{\frac{p-1}{2^j}}$ until you get -1 or $n^{2k+1} \mod p = 1$

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k + 1)$.
4. Note: $n^{\frac{p-1}{4}} \mod p = \pm 1$. Repeat calculating $n^{\frac{p-1}{2^j}}$ until you get -1 or $n^{2k+1} \mod p = 1$
5. If $n^{\frac{p-1}{2^j}} = -1$ then find a non-quadratic residue β that is $\beta^{\frac{p-1}{2}} \mod p = -1$ (easy, just try a few numbers).

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k+1)$.
4. Note: $n^{\frac{p-1}{4}} \mod p = \pm 1$. Repeat calculating $n^{\frac{p-1}{2^j}}$ until you get -1 or $n^{2k+1} \mod p = 1$
5. If $n^{\frac{p-1}{2^j}} = -1$ then find a non-quadratic residue β that is $\beta^{\frac{p-1}{2}} \mod p = -1$ (easy, just try a few numbers).
6. $n^{\frac{p-1}{2^j}} \beta^{\frac{p-1}{2}} \mod p = 1$

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k + 1)$.
4. Note: $n^{\frac{p-1}{4}} \mod p = \pm 1$. Repeat calculating $n^{\frac{p-1}{2^j}}$ until you get -1 or $n^{2k+1} \mod p = 1$
5. If $n^{\frac{p-1}{2^j}} = -1$ then find a non-quadratic residue β that is $\beta^{\frac{p-1}{2}} \mod p = -1$ (easy, just try a few numbers).
6. $n^{\frac{p-1}{2^j}} \beta^{\frac{p-1}{2}} \mod p = 1$
7. Calculate: $n^{\frac{p-1}{2^{j+1}}} \beta^{\frac{p-1}{4}} \mod p = \pm 1$

$\sqrt{n} \mod p$

1. Calculate $n^{\frac{p-1}{2}} \mod p = \pm 1$ (use one of the powermod functions).
2. If $n^{\frac{p-1}{2}} \mod p = -1$ stop! n is not a quadratic residue.
3. Let $p - 1 = 2^m(2k + 1)$.
4. Note: $n^{\frac{p-1}{4}} \mod p = \pm 1$. Repeat calculating $n^{\frac{p-1}{2^j}}$ until you get -1 or $n^{2k+1} \mod p = 1$
5. If $n^{\frac{p-1}{2^j}} = -1$ then find a non-quadratic residue β that is $\beta^{\frac{p-1}{2}} \mod p = -1$ (easy, just try a few numbers).
6. $n^{\frac{p-1}{2^j}} \beta^{\frac{p-1}{2}} \mod p = 1$
7. Calculate: $n^{\frac{p-1}{2^{j+1}}} \beta^{\frac{p-1}{4}} \mod p = \pm 1$
8. Repeat the same process ubtil you reach $n^{2k+1} \beta^{2s} \mod p = 1$

Examples

Example

Examples

Example

1. $p = 3 \bmod 4$.

Examples

Example

1. $p = 3 \mod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.

Examples

Example

1. $p = 3 \bmod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.

Examples

Example

1. $p = 3 \bmod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.
3. - *Let* $p = 337639$.

Examples

Example

1. $p = 3 \bmod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.
3. - *Let* $p = 337639$.
     $71^{168819} \bmod 337639 = 1$ *(71 is a quadratic residue mod 337639).*

Examples

Example

1. $p = 3 \bmod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.
3. - *Let* $p = 337639$.
     $71^{168819} \bmod 337639 = 1$ *(71 is a quadratic residue mod 337639).*
     $71^{168820/2} \bmod 337639 = 234428$.

Examples

Example

1. $p = 3 \bmod 4$.
2. *This is a very easy case as* $\frac{p-1}{2} = 2k+1, \quad n^{2k+1} \bmod p = 1$ *so* $\sqrt{n} \bmod p = n^{k+1}$.
3. - *Let* $p = 337639$.
     $71^{168819} \bmod 337639 = 1$ *(71 is a quadratic residue mod 337639).*
     $71^{168820/2} \bmod 337639 = 234428$.
     $234428^2 \bmod 337639 = 71$.
     So $\sqrt{71} \bmod 337639 = 234428$.

1. $p = 2701297,\ p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37$.
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37$.
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37$.
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1$.

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1.$
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1.$
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$
6. $75^{(p-1)/8} 71^{(p-1)/4} \bmod p = -1 \Rightarrow$
   $75^{(p-1)/8} 71^{3(p-1)/4} \bmod p = 1.$

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1.$
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$
6. $75^{(p-1)/8} 71^{(p-1)/4} \bmod p = -1 \Rightarrow$ $75^{(p-1)/8} 71^{3(p-1)/4} \bmod p = 1.$
7. $75^{(p-1)/16} 71^{3(p-1)/8} = 75^{168331} 71^{1012986} \bmod p = 1$

1. $p = 2701297,\ p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1.$
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$
6. $75^{(p-1)/8} 71^{(p-1)/4} \bmod p = -1 \Rightarrow$ $75^{(p-1)/8} 71^{3(p-1)/4} \bmod p = 1.$
7. $75^{(p-1)/16} 71^{3(p-1)/8} = 75^{168331} 71^{1012986} \bmod p = 1$
8. $\sqrt{75} \bmod p = 75^{168332/2} 71^{1012986/2} \bmod p = 2309891$

1. $p = 2701297, \; p - 1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37$.
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1$.
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$
6. $75^{(p-1)/8} 71^{(p-1)/4} \bmod p = -1 \Rightarrow$ $75^{(p-1)/8} 71^{3(p-1)/4} \bmod p = 1$.
7. $75^{(p-1)/16} 71^{3(p-1)/8} = 75^{168331} 71^{1012986} \bmod p = 1$
8. $\sqrt{75} \bmod p = 75^{168332/2} 71^{1012986/2} \bmod p = 2309891$
9. Verify: $2309891^2 \bmod p = 75$.

1. $p = 2701297, \; p-1 = 2^4 \cdot 3^3 \cdot 13^2 \cdot 37.$
2. $71^{(p-1)/2} = 2701296$ so 71 is not a quadratic residue mod p.
3. 75 is a quadratic residue.
4. $75^{(p-1)/4} \bmod p = 2701296 = -1.$
5. $71^{(p-1)/2} \bmod p = -1 \Rightarrow 75^{(p-1)/4} 71^{(p-1)/2} \bmod p = 1$
6. $75^{(p-1)/8} 71^{(p-1)/4} \bmod p = -1 \Rightarrow$
   $75^{(p-1)/8} 71^{3(p-1)/4} \bmod p = 1.$
7. $75^{(p-1)/16} 71^{3(p-1)/8} = 75^{168331} 71^{1012986} \bmod p = 1$
8. $\sqrt{75} \bmod p = 75^{168332/2} 71^{1012986/2} \bmod p = 2309891$
9. Verify: $2309891^2 \bmod p = 75.$
10. We can verify it in yet another way. $75 = 25 \cdot 3$. This means that $\sqrt{3} \bmod p \; = 2309891/5$. Indeed $5^{-1} \bmod p = 1080519$ and $1080519 \cdot 2309891 \bmod p = 1542497$ *and* $1542497^2 \bmod p = 3$.