Discrete Mathematics
Lecture-15

Ngày 9 tháng 12 năm 2011

Security 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.

Security 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.

Security 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.

Security 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

How to design a system with the following properties was a problem scientists faced:

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

How to design a system with the following properties was a problem scientists faced:

- *Participants can securely exchange messages 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

How to design a system with the following properties was a problem scientists faced:

- *Participants can securely exchange messages over an "open" system.*
- *Messages can be sent to "Bob" so only Bob will be able to understand.*

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

How to design a system with the following properties was a problem scientists faced:

- *Participants can securely exchange messages over an "open" system.*
- *Messages can be sent to "Bob" so only Bob will be able to understand.*
- *Transactions can 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.

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.

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.

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

the 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.

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)

the 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.

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)

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

the 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.

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)

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

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

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.
- Every participant in the communication network has a **key.**

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.
- Every participant in the communication network has a **key**.
- The key consists of two parts:
  Public part: $\{k, e\}$ where k, e are integers.

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.
- Every participant in the communication network has a **key**.
- The key consists of two parts:
  Public part: $\{k, e\}$ where k, e are integers.
- Private part: $k = p \cdot q,\ gcd(e, (p-1)(q-1)) = 1$.
  Only the owner of the key knows p *and* q.

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.
- Every participant in the communication network has a **key**.
- The key consists of two parts:
  Public part: $\{k, e\}$ where k, e are integers.
- Private part: $k = p \cdot q,\ gcd(e, (p-1)(q-1)) = 1$.
  Only the owner of the key knows p *and* q.
- Encryption: to send a message M to the owner of the key (k, e) the sender calculates:

$$S = M^e \bmod k \text{ and sends } S.$$

The RSA public key system

- Every message is a binary sequence, thus can be viewed as an integer.
- Every participant in the communication network has a **key.**
- The key consists of two parts:
  Public part: $\{k, e\}$ where k, e are integers.
- Private part: $k = p \cdot q,\ gcd(e, (p-1)(q-1)) = 1$.
  Only the owner of the key knows p *and* q.
- Encryption: to send a message M to the owner of the key (k, e) the sender calculates:

$$S = M^e \bmod k \text{ and sends } S.$$

- Decryption: the receiver calculates $S^d \bmod k$ and retrieves M where $d = e^{(-1)} \bmod (p-1)(q-1)$.

Decryption

$$d = e^{(-1)} \bmod (p-1)(q-1) \Longrightarrow d \cdot e = a \cdot (p-1)(q-1) + 1$$

Decryption

$d = e^{(-1)} \bmod (p-1)(q-1) \Longrightarrow d \cdot e = a \cdot (p-1)(q-1) + 1$

$S^d \bmod k = M^{ed} \bmod k = M^{a(p-1)(q-1)+1} \bmod p \cdot q =$
$M \cdot (M^{\phi(pq)})^a \bmod p \cdot q = M \bmod p \cdot q = M.$

Decryption

$d = e^{(-1)} \bmod (p-1)(q-1) \Longrightarrow d \cdot e = a \cdot (p-1)(q-1) + 1$

$S^d \bmod k = M^{ed} \bmod k = M^{a(p-1)(q-1)+1} \bmod p \cdot q =$
$M \cdot (M^{\phi(pq)})^a \bmod p \cdot q = M \bmod p \cdot q = M.$

In order to calculate $e^{(-1)} \bmod (p-1)(q-1)$ we need to know $(p-1)(q-1)$ but finding this number if we only know the product $k (= pq)$ is equivalent to being able to factor k

Decryption

$d = e^{(-1)} \bmod (p-1)(q-1) \Longrightarrow d \cdot e = a \cdot (p-1)(q-1) + 1$

$S^d \bmod k = M^{ed} \bmod k = M^{a(p-1)(q-1)+1} \bmod p \cdot q =$
$M \cdot (M^{\phi(pq)})^a \bmod p \cdot q = M \bmod p \cdot q = M.$

In order to calculate $e^{(-1)} \bmod (p-1)(q-1)$ we need to know $(p-1)(q-1)$ but finding this number if we only know the product $k(= pq)$ is equivalent to being able to factor k

So the question is how difficult it is to factor integers?

Decryption

$d = e^{(-1)} \bmod (p-1)(q-1) \Longrightarrow d \cdot e = a \cdot (p-1)(q-1) + 1$

$S^d \bmod k = M^{ed} \bmod k = M^{a(p-1)(q-1)+1} \bmod p \cdot q =$
$M \cdot (M^{\phi(pq)})^a \bmod p \cdot q = M \bmod p \cdot q = M.$

In order to calculate $e^{(-1)} \bmod (p-1)(q-1)$ we need to know $(p-1)(q-1)$ but finding this number if we only know the product $k(=pq)$ is equivalent to being able to factor k

So the question is how difficult it is to factor integers?

Security experts all over the world are trying hard to devise methods to factor large integers quickly. So far their efforts have not succeeded.

Decryption

$d = e^{(-1)} \bmod (p-1)(q-1) \implies d \cdot e = a \cdot (p-1)(q-1) + 1$

$S^d \bmod k = M^{ed} \bmod k = M^{a(p-1)(q-1)+1} \bmod p \cdot q =$
$M \cdot (M^{\phi(pq)})^a \bmod p \cdot q = M \bmod p \cdot q = M.$

In order to calculate $e^{(-1)} \bmod (p-1)(q-1)$ we need to know $(p-1)(q-1)$ but finding this number if we only know the product $k(= pq)$ is equivalent to being able to factor k

So the question is how difficult it is to factor integers?

Security experts all over the world are trying hard to devise methods to factor large integers quickly. So far their efforts have not succeeded.

We shall devote the rest of our time to take a quick glimpse at factoring.

Discussion

Note: we assume that everyone can intercept the message S. Furthermore, everyone knows exactly how S was calculated, everyone knows k and e, so why can't they retrieve M?

Discussion

Note: we assume that everyone can intercept the message S. Furthermore, everyone knows exactly how S was calculated, everyone knows k and e, so why can't they retrieve M?

Discussion

Note: we assume that everyone can intercept the message S. Furthermore, everyone knows exactly how S was calculated, everyone knows k and e, so why can't they retrieve M?

After all, all they need to do is calculate $d = e^{(-1)} \bmod (p-1)(q-1)$ and in order to do it they just need to factor k.

Our goal is to understand how this system works, why it is considered secure and other applications of this system.

Discussion

Note: we assume that everyone can intercept the message S. Furthermore, everyone knows exactly how S was calculated, everyone knows k and e, so why can't they retrieve M?

After all, all they need to do is calculate $d = e^{(-1)} \bmod (p-1)(q-1)$ and in order to do it they just need to factor k.

Our goal is to understand how this system works, why it is considered secure and other applications of this system.

To understand it we need to study some very mathematically interesting topics in modular arithmetic.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.
- For each prime p and positive integer n there is a field $GF(p^n)$ with p^n elements.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.
- For each prime p and positive integer n there is a field $GF(p^n)$ with p^n elements.
- **Definition:**
  An element $\alpha \in GF(q)$ is **primitive** if
  $\{\alpha^i \mid 0 \leq i \leq q-2\} = GF^*(q);\ GF^*(q) = GF(q) \setminus \{0\}$.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.
- For each prime p and positive integer n there is a field $GF(p^n)$ with p^n elements.
- **Definition:**
  An element $\alpha \in GF(q)$ is **primitive** if
  $\{\alpha^i \mid 0 \leq i \leq q-2\} = GF^*(q);\ GF^*(q) = GF(q) \setminus \{0\}$.
- **Theorem:** Every finite field has primitive elements.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.
- For each prime p and positive integer n there is a field $GF(p^n)$ with p^n elements.
- **Definition:**
  An element $\alpha \in GF(q)$ is **primitive** if
  $\{\alpha^i \mid 0 \leq i \leq q-2\} = GF^*(q);\ GF^*(q) = GF(q) \setminus \{0\}$.
- **Theorem:** Every finite field has primitive elements.
- If $p(x)$ is a polynomial with coefficients in $GF(q)$ and $p(k) = 0$ then $p(x) = (x-k)p_1(x)$.

Prime and not primes, some key facts

- In this discussion p is assumed to be a prime number.
- $GF(p) = \{0, 1, \ldots, p-1\}$ is a field, arithmetic done mod p.
- For each prime p and positive integer n there is a field $GF(p^n)$ with p^n elements.
- **Definition:**
  An element $\alpha \in GF(q)$ is **primitive** if
  $\{\alpha^i \mid 0 \le i \le q-2\} = GF^*(q);\ GF^*(q) = GF(q) \setminus \{0\}$.
- **Theorem:** Every finite field has primitive elements.
- If $p(x)$ is a polynomial with coefficients in $GF(q)$ and $p(k) = 0$ then $p(x) = (x-k)p_1(x)$.
- A polynomial $p(x)$ of degree k over $GF(q)$ has at most k roots.

Primality testing

To build an RSA cryptosystem we need to be able to test whether given numbers are prime and to “manufacture” large primes. We shall start by testing.

Primality testing

To build an RSA cryptosystem we need to be able to test whether given numbers are prime and to “manufacture” large primes. We shall start by testing.

Question

Can Fermat’s theorem be used for testing primality?

Primality testing

To build an RSA cryptosystem we need to be able to test whether given numbers are prime and to "manufacture" large primes. We shall start by testing.

Question

Can Fermat's theorem be used for testing primality?

Answer

Unfortunately not. There are numbers for which the chances for finding an integer $a < n$ such that $a^{(n-1)} \bmod n \neq 1$ are very slim.
For instance if $n = (6k+1)(12k+1)(18k+1)$ and $(6k+1), (12k+1)$ and $(18k+1)$ are prime, then if $gcd(a, n) = 1$ $a^{n-1} \bmod n = 1$.

Primality testing

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.

Primality testing

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 $a^{N-1} \bmod N = 1$?

Primality testing

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

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

Answer: NOTHING! N may be prime and it may be composite! At best, we can try another integer a.

Example

As we noted in our drill, k^{1728} mod $1729 = 1$ *for all* $k,\ gcd(k, 1729) = 1$*. Our chances to randomly select k such that* $gcd(k, 1729) > 1$ *are very slim.*

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ *such that* $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a \text{ such that } gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ *such that* $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

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

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ such that $gcd(a, N) = 1$ are called **Carmichael numbers***.*

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer, $N - 1 = 2^m \cdot (2k + 1)$.*
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a \text{ such that } gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer,* $N - 1 = 2^m \cdot (2k + 1)$.
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*
- *For some* $1 \leq i \leq m \quad w^{2^i \cdot (2k+1)} = -1$

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ *such that* $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer,* $N - 1 = 2^m \cdot (2k + 1)$.
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*
- *For some* $1 \leq i \leq m \quad w^{2^i \cdot (2k+1)} = -1$
- *Or:* $w^{2^i \cdot (2k+1)} \bmod (N) = 1$ *and* $w^{2k+1} = \pm 1$.

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ *such that* $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer,* $N - 1 = 2^m \cdot (2k + 1)$.
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*
- *For some* $1 \leq i \leq m \quad w^{2^i \cdot (2k+1)} = -1$
- *Or:* $w^{2^i \cdot (2k+1)} \bmod (N) = 1$ *and* $w^{2k+1} = \pm 1$.

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ such that $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer,* $N - 1 = 2^m \cdot (2k + 1)$.
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*
- *For some* $1 \leq i \leq m \quad w^{2^i \cdot (2k+1)} = -1$
- *Or:* $w^{2^i \cdot (2k+1)} \bmod (N) = 1$ *and* $w^{2k+1} = \pm 1$.

In other words, the test fails to determine whether N is composite.

The Miller-Rabin Primality Test

Comment

Positive integers N for which $a^{N-1} \bmod N = 1$ $\forall a$ *such that* $gcd(a, N) = 1$ *are called* **Carmichael numbers**.

There are infinitely many Carmichael numbers.

Theorem (The Miller-Rabin Test)

- *Let N be an odd positive integer,* $N - 1 = 2^m \cdot (2k + 1)$.
- *An integer w is* **NOT** *a "witnesses" that N is composite if:*
- *For some* $1 \leq i \leq m \quad w^{2^i \cdot (2k+1)} = -1$
- *Or:* $w^{2^i \cdot (2k+1)} \bmod (N) = 1$ *and* $w^{2k+1} = \pm 1$.

In other words, the test fails to determine whether N is composite. (Do you know another example of a "failing" test?)

Chứng minh.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.
- If $w^{(N-1)/2} \bmod N = 1$ we calculate $w^{(N-1)/4} \bmod N = \pm 1$.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.
- If $w^{(N-1)/2} \bmod N = 1$ we calculate $w^{(N-1)/4} \bmod N = \pm 1$.
- As long as the results of $w^{(N-1)/2^i} \bmod N = 1$ we continue until we reach w^{2k+1}.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.
- If $w^{(N-1)/2} \bmod N = 1$ we calculate $w^{(N-1)/4} \bmod N = \pm 1$.
- As long as the results of $w^{(N-1)/2^i} \bmod N = 1$ we continue until we reach w^{2k+1}.
- If $w^{2k+1} \bmod N \neq \pm 1$ then N is definitely composite.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.
- If $w^{(N-1)/2} \bmod N = 1$ we calculate $w^{(N-1)/4} \bmod N = \pm 1$.
- As long as the results of $w^{(N-1)/2^i} \bmod N = 1$ we continue until we reach w^{2k+1}.
- If $w^{2k+1} \bmod N \neq \pm 1$ then N is definitely composite.

□

Chứng minh.

- If N is prime then $w^{N-1} \bmod N = 1$ (Fermat).
- So $w^{(N-1)/2} \bmod N = \pm 1$.
- If $w^{(N-1)/2} \bmod N = -1$ the test stops. it is inconclusive.
- If $w^{(N-1)/2} \bmod N = 1$ we calculate $w^{(N-1)/4} \bmod N = \pm 1$.
- As long as the results of $w^{(N-1)/2^i} \bmod N = 1$ we continue until we reach w^{2k+1}.
- If $w^{2k+1} \bmod N \neq \pm 1$ then N is definitely composite.

□

We skip the important part of the proof: more than 50% of the integers $a < N$ are composite-witnesses. So, to test whether an integer p is prime, randomly select 100 integers $a < p$, apply to them the Miller-Rabin test. If the test fails, we assume that p is prime. The probabilty that we made a mistake, that is declared p is prime while it is not, is less than $(\frac{1}{2})^{100}$ which is far less that the probability that the computer will make a mistake.

Example

Example

- *1729 is a composite integer.*

Example

- 1729 *is a composite integer.*
- $1728 = 2^6 \cdot 3^3$.

Example

- 1729 *is a composite integer.*
- $1728 = 2^6 \cdot 3^3$.
- $3^{2^i \cdot 3^3} = \mod 1729 = 1$ *for* $1 \leq i \leq 6$.

Example

- 1729 *is a composite integer.*
- $1728 = 2^6 \cdot 3^3$.
- $3^{2^i \cdot 3^3} = \mod 1729 = 1$ *for* $1 \leq i \leq 6$.
- *But* $3^{3^3} = 664$ *proving that* 1729 *is composite.*

Example

- 1729 *is a composite integer.*
- $1728 = 2^6 \cdot 3^3$.
- $3^{2^i \cdot 3^3} = \mod 1729 = 1$ *for* $1 \leq i \leq 6$.
- *But* $3^{3^3} = 664$ *proving that* 1729 *is composite.*
- *Drill: Find a witness that will prove that* 413138881 *is composite.*

Factoring large integers

- The inventors of RSA published in 1977 an integer called RSA-129 (129 digits long) and chelleneged the public to factor it.

Factoring large integers

- The inventors of RSA published in 1977 an integer called RSA-129 (129 digits long) and chelleneged the public to factor it.
- $RSA - 129 =$
  1143816257578888676692357799761466120102182967212422562561842935706935245733897830597123563958705058989075147599290026879543541.

Factoring large integers

- The inventors of RSA published in 1977 an integer called RSA-129 (129 digits long) and chelleneged the public to factor it.
- $RSA - 129 =$ 114381625757888867669235779976146612010218296721242 362562561842935706935245733897830597123563958705058989 0751475992900268795435 41.
- RSA-129 was factored in April 1994 (17 years later) by a team led by Derek Atkins, Michael Graff, Arjen K. Lenstra and Paul Leyland, using approximately 1600 computers from around 600 volunteers.

Factoring large integers

- The inventors of RSA published in 1977 an integer called RSA-129 (129 digits long) and chelleneged the public to factor it.
- $RSA - 129 =$ 1143816257578888676692357799761466120102182967212422562561842935706935245733897830597123563958705058989075147599290026879543541.
- RSA-129 was factored in April 1994 (17 years later) by a team led by Derek Atkins, Michael Graff, Arjen K. Lenstra and Paul Leyland, using approximately 1600 computers from around 600 volunteers.
- $RSA - 129 =$ 3490529510847650949147849619903898133417764638493387843990820577 $\times$ 32769132993266709549961988190834461413177642967992942539798288533

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.
- There is a $\$100,000$ USD prize offered for its factorization.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.
- There is a $\$100,000$ USD prize offered for its factorization.
- It is of particular interest as this is the current size used in applications.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.
- There is a $\$100,000$ USD prize offered for its factorization.
- It is of particular interest as this is the current size used in applications.
- R-2048 (617 decimal digits) has a prize of $\$200,000$ USD for its factors.

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.
- There is a $\$100,000$ USD prize offered for its factorization.
- It is of particular interest as this is the current size used in applications.
- R-2048 (617 decimal digits) has a prize of $\$200,000$ USD for its factors.
- The largest RSA number factored so far is RSA-768 (232 decimal digits).

Can you make money factoring integers?

- The RSA corporation published many integers and challenged the public to factor them.
- Almost all the RSA numbers with more than 250 digits have not been factored yet.
- RSA-1024 (2^{10} bits or 309 decimal digits) has not been factored.
- There is a $\$100,000$ USD prize offered for its factorization.
- It is of particular interest as this is the current size used in applications.
- R-2048 (617 decimal digits) has a prize of $\$200,000$ USD for its factors.
- The largest RSA number factored so far is RSA-768 (232 decimal digits).
- RSA-200 was factored in 2009. The CPU time spent by computers working in parallel on this factorization was equivalent to about 75 years of CPU time on a 2.2GHz single processor.

- To implement the RSA cryptosystem we need to produce large prime numbers.

- To implement the RSA cryptosystem we need to produce large prime numbers.
- The Miller-Rabin test was commonly used to manufacture large primes.

- To implement the RSA cryptosystem we need to produce large prime numbers.
- The Miller-Rabin test was commonly used to manufacture large primes.
- There are efficient algorithms that can manufacture “certified” large primes.

- To implement the RSA cryptosystem we need to produce large prime numbers.
- The Miller-Rabin test was commonly used to manufacture large primes.
- There are efficient algorithms that can manufacture “certified” large primes.
- In today’s implemenatations, keys with 309 digits are being used.

- To implement the RSA cryptosystem we need to produce large prime numbers.
- The Miller-Rabin test was commonly used to manufacture large primes.
- There are efficient algorithms that can manufacture “certified” large primes.
- In today’s implemenatations, keys with 309 digits are being used.
- Are all large primes “safe”?

- To implement the RSA cryptosystem we need to produce large prime numbers.
- The Miller-Rabin test was commonly used to manufacture large primes.
- There are efficient algorithms that can manufacture “certified” large primes.
- In today’s implemenatations, keys with 309 digits are being used.
- Are all large primes “safe”?
- Not really. There are some very sofisticated attacks on “weak” primes.

Square roots and factoring

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 and factoring

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.

We shall show that finding $\sqrt{n} \bmod k$ is as difficult as factoring k. That is if we had an algorithm that could effciently find $\sqrt{n} \bmod k$ then we could factor k.

Square roots and factoring

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.

We shall show that finding $\sqrt{n}$ mod k is as difficult as factoring k. That is if we had an algorithm that could effciently find $\sqrt{n}$ mod k then we could factor k.

Definition

$r \in GF*(q)$ is a **quadratic-residue mod q** *if there is an $s \in GF(q)$ such that $s^2 = r$.*

We shall start with the easy task: finding $\sqrt{n}$ mod p, p is prime.

Square roots and factoring

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.

We shall show that finding $\sqrt{n} \bmod k$ is as difficult as factoring k. That is if we had an algorithm that could effciently find $\sqrt{n} \bmod k$ then we could factor k.

Definition

$r \in GF*(q)$ is a **quadratic-residue mod q** *if there is an $s \in GF(q)$ such that $s^2 = r$.*

We shall start with the easy task: finding $\sqrt{n} \bmod p,\ p$ is prime.

Square roots and factoring

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.

We shall show that finding $\sqrt{n} \bmod k$ is as difficult as factoring k. That is if we had an algorithm that could effciently find $\sqrt{n} \bmod k$ then we could factor k.

Definition

$r \in GF*(q)$ is a **quadratic-residue mod q** *if there is an $s \in GF(q)$ such that $s^2 = r$.*

We shall start with the easy task: finding $\sqrt{n} \bmod p,\ p$ is prime.

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.

$\sqrt{n}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

$\sqrt{\mathbf{n}}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

Calcuate $n^{(p-1)/2}$ mod p.

Note: $n = \alpha^m$ where α is a primitive number mod$p$.
n is a quadratic residue mod$p$ if and only if $m = 2k$.

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

Note: $n = \alpha^m$ where α is a primitive number mod$p$.
n is a quadratic residue mod$p$ if and only if $m = 2k$.

($\sqrt{n}$ mod p, $\quad p = 4k + 3$)

$\sqrt{\mathbf{n}}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

Note: $n = \alpha^m$ where α is a primitive number mod$p$.
n is a quadratic residue mod$p$ if and only if $m = 2k$.

($\sqrt{n}$ mod p, $\quad p = 4k + 3$)

- *Calculate* $a = n^{2k+1} \bmod p$.

$\sqrt{n}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

Note: $n = \alpha^m$ where α is a primitive number mod$p$.
n is a quadratic residue mod$p$ if and only if $m = 2k$.

($\sqrt{n}$ mod p, $\quad p = 4k + 3$)

- *Calculate* $a = n^{2k+1} \bmod p$.
- *If* $a = -1$ *stop, n does not have a square root* mod$p$.

$\sqrt{n}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

Note: $n = \alpha^m$ where α is a primitive number mod p.
n is a quadratic residue mod p if and only if $m = 2k$.

($\sqrt{n}$ mod p, $p = 4k + 3$)

- *Calculate* $a = n^{2k+1} \bmod p$.
- *If* $a = -1$ *stop,* n *does not have a square root* mod p.
- $n^{2k+1} = 1 \bmod p \Longrightarrow n^{2k+2} \bmod p = n$.

$\sqrt{n}$ mod p

Testing whether an integer n is a quadratic residue mod p is easy:

$$\text{Calcuate } n^{(p-1)/2} \bmod p.$$

Note: $n = \alpha^m$ where α is a primitive number mod p.
n is a quadratic residue mod p if and only if $m = 2k$.

($\sqrt{n} \bmod p, \quad p = 4k + 3$)

- *Calculate* $a = n^{2k+1} \bmod p$.
- *If* $a = -1$ *stop, n does not have a square root* mod p.
- $n^{2k+1} = 1 \bmod p \Longrightarrow n^{2k+2} \bmod p = n$.
- $\sqrt{n} \bmod p = n^{k+1} \bmod p$.

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod 337639 = 234428)$

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod \ 337639 = 234428)$

$(\sqrt{n} \bmod p, \quad p = 4k + 1)$

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod\ 337639 = 234428)$

($\sqrt{n} \bmod p, \quad p = 4k + 1$)

- *Calculate $a = n^{2k} \bmod p$.*

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod 337639 = 234428)$

$(\sqrt{n} \bmod p, \quad p = 4k + 1)$

- *Calculate $a = n^{2k} \bmod p$.*
- *If $a = -1$ stop, n does not have a square root $\bmod p$.*

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod\ 337639 = 234428)$

($\sqrt{n} \bmod p, \quad p = 4k+1$)

- *Calculate $a = n^{2k} \bmod p$.*
- *If $a = -1$ stop, n does not have a square root* mod *p.*
- *Let $p - 1 = 2^k(2m+1)$.*

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod \ 337639 = 234428)$

($\sqrt{n} \bmod p, \quad p = 4k + 1$)

- *Calculate $a = n^{2k} \bmod p$.*
- *If $a = -1$ stop, n does not have a square root $\bmod p$.*
- *Let $p - 1 = 2^k(2m + 1)$.*
- *If we can find an odd integer such that $a^{2s+1} b^{2t} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{s+1} \cdot b^t \bmod p$.*

Examples

- Let $p = 337639$. This is a prime. $337639 = 4 \cdot 84409 + 3$.
- $71^{168819} \bmod 337639 = 1$.
  So 71 has a square root mod 337639.
- $71^{168820/2} \bmod 337639 = 234428$.
- Testing:
  $234428^2 \bmod 337639 = 71 (\sqrt{71} \bmod 337639 = 234428)$

($\sqrt{n} \bmod p, \quad p = 4k + 1$)

- *Calculate* $a = n^{2k} \bmod p$.
- *If* $a = -1$ *stop, n does not have a square root* mod p.
- *Let* $p - 1 = 2^k(2m + 1)$.
- *If we can find an odd integer such that* $a^{2s+1} b^{2t} \bmod p = 1$ *then* $\sqrt{a} \bmod p = a^{s+1} \cdot b^t \bmod p$.
- *This can be accomplished as follows:*

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.
- This is easy. Note that $b^{2^{k-1}(2m+1)} \bmod p = -1$ so:

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.
- This is easy. Note that $b^{2^{k-1}(2m+1)} \bmod p = -1$ so:
- $a^{2^d(2m+1)} \mathrm{b}^{2^{k-1}(2m+1)} \bmod p = 1$

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.
- This is easy. Note that $b^{2^{k-1}(2m+1)} \bmod p = -1$ so:
- $a^{2^d(2m+1)} \mathrm{b}^{2^{k-1}(2m+1)} \bmod p = 1$
- We can repeat reducing the exponent by a factor of 2, multiplying by b to make sure that the product will remain 1 until we reach $a^{2k+1} b^{2j} \bmod p = 1$.

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.
- This is easy. Note that $b^{2^{k-1}(2m+1)} \bmod p = -1$ so:
- $a^{2^d(2m+1)}\mathrm{b}^{2^{k-1}(2m+1)} \bmod p = 1$
- We can repeat reducing the exponent by a factor of 2, multiplying by b to make sure that the product will remain 1 until we reach $a^{2k+1}b^{2j} \bmod p = 1$.
- $\sqrt{n} \bmod p = a^{k+1}b^{j} \bmod p$.

- While $a^{2^d(2m+1)} \bmod p = 1$ do: $d = d - 1$.
- This loop will terminate either when $a^{2^d(2m+1)} \bmod p = -1$ or $a^{2m+1} \bmod p = 1$
- If $a^{2m+1} \bmod p = 1$ then $\sqrt{a} \bmod p = a^{m+1} \bmod p$.
- If $a^{2^d(2m+1)} \bmod p = -1$ then find b, a non-quadratic residue mod p.
- This is easy. Note that $b^{2^{k-1}(2m+1)} \bmod p = -1$ so:
- $a^{2^d(2m+1)} \mathrm{b}^{2^{k-1}(2m+1)} \bmod p = 1$
- We can repeat reducing the exponent by a factor of 2, multiplying by b to make sure that the product will remain 1 until we reach $a^{2k+1} b^{2j} \bmod p = 1$.
- $\sqrt{n} \bmod p = a^{k+1} b^j \bmod p$.
- For an example see the SAGE sample in the supplements folder.

$\sqrt{n} \bmod p \cdot q$

See the file factoring.pdf