Factoring

Ngày 13 tháng 12 năm 2010

Question

How difficult is factoring? Conceptually, this is a very simple operation. To factor an integer n just test whether a prime $p < n$ divides n. All we have to do is test the primes $p < \lfloor\sqrt{n}\rfloor$.

Factoring

Question

How difficult is factoring? Conceptually, this is a very simple operation. To factor an integer n just test whether a prime $p < n$ divides n. All we have to do is test the primes $p < \lfloor\sqrt{n}\rfloor$.

Factoring

Question

How difficult is factoring? Conceptually, this is a very simple operation. To factor an integer n just test whether a prime $p < n$ divides n. All we have to do is test the primes $p < \lfloor\sqrt{n}\rfloor$.

How difficult can this be?

Answer

Very difficult. In applications we use integers that are 200 digits long. The number of primes smaller than $\sqrt{n}$ is about $\frac{2\sqrt{n}}{\log n}$ which is a number with a little less than 100 digits. Way too big for any computer we have today.

Factoring

Question

How difficult is factoring? Conceptually, this is a very simple operation. To factor an integer n just test whether a prime $p < n$ divides n. All we have to do is test the primes $p < \lfloor\sqrt{n}\rfloor$.

How difficult can this be?

Answer

Very difficult. In applications we use integers that are 200 digits long. The number of primes smaller than $\sqrt{n}$ is about $\frac{2\sqrt{n}}{\log\ n}$ which is a number with a little less than 100 digits. Way too big for any computer we have today.

Question

So how safe is our reliance on factoring for our cryptosystems?

1. **Observation:**

1. **Observation:**
2. $4^2 \bmod 77 = 16$

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$
5. $59^2 \bmod 77 = (77-18)^2 \bmod 77 = (-18)^2 \bmod 77 = 16.$

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$
5. $59^2 \bmod 77 = (77-18)^2 \bmod 77 = (-18)^2 \bmod 77 = 16.$
6. Looks as if 16 has 4 distinct square roots mod 77.

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$
5. $59^2 \bmod 77 = (77-18)^2 \bmod 77 = (-18)^2 \bmod 77 = 16.$
6. Looks as if 16 has 4 distinct square roots mod 77.

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$
5. $59^2 \bmod 77 = (77-18)^2 \bmod 77 = (-18)^2 \bmod 77 = 16.$
6. Looks as if 16 has 4 distinct square roots mod 77.

Coincidence?

1. **Observation:**
2. $4^2 \bmod 77 = 16$
3. $73^2 = (77-4)^2 \bmod 77 = (-4)^2 \bmod 77 = 16.$
4. $18^2 \bmod 77 = 324 \bmod 77 = 4 \cdot 77 + 16 \bmod 77 = 16$
5. $59^2 \bmod 77 = (77-18)^2 \bmod 77 = (-18)^2 \bmod 77 = 16.$
6. Looks as if 16 has 4 distinct square roots mod 77.

Coincidence?

Theorem

If $n = p \cdot q$ and k is a quadratic residue mod *n then k has four distinct square roots* mod *n.*

Chứng minh.

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q$.

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q$.
5. Claim: $(\pm apx \pm bqx)^2 = k \bmod pq$ (Note: these are four distinct numbers).

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q$.
5. Claim: $(\pm apx \pm bqx)^2 = k \bmod pq$ (Note: these are four distinct numbers).
   - $(apx - bqx)^2 \bmod p = (bqx)^2 \bmod p = (apx + bqx)^2 \bmod p = x^2 \bmod p = k$

Chứng minh.

1. p,q are distinct primes so $GCD(p,q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q$.
5. Claim: $(\pm apx \pm bqx)^2 = k \bmod pq$ (Note: these are four distinct numbers).
   - $(apx - bqx)^2 \bmod p = (bqx)^2 \bmod p = (apx + bqx)^2 \bmod p = x^2 \bmod p = k$
   - Similarly, $(apx - bqx)^2 \bmod q = k$

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q.$
5. Claim: $(\pm apx \pm bqx)^2 = k \bmod pq$ (Note: these are four distinct numbers).
   - $(apx - bqx)^2 \bmod p = (bqx)^2 \bmod p = (apx + bqx)^2 \bmod p = x^2 \bmod p = k$
   - Similarly, $(apx - bqx)^2 \bmod q = k$
   - By the Chinese Reamainder Theorem $(apx - bqx)^2 \bmod pq = k$.

$\square$

Chứng minh.

1. p,q are distinct primes so $GCD(p, q) = 1$.
2. Let $ap + bq = 1$ (Extended GCD).
3. Let k be a quadratic residue mod $p \cdot q$ that is $k = x^2 + m \cdot p \cdot q$
4. $k = x^2 \bmod p, \quad k = x^2 \bmod q.$
5. Claim: $(\pm apx \pm bqx)^2 = k \bmod pq$ (Note: these are four distinct numbers).
   - $(apx - bqx)^2 \bmod p = (bqx)^2 \bmod p = (apx + bqx)^2 \bmod p = x^2 \bmod p = k$
   - Similarly, $(apx - bqx)^2 \bmod q = k$
   - By the Chinese Reamainder Theorem $(apx - bqx)^2 \bmod pq = k$.
   - The proof for the other three numbers is the same.

$\square$

Example

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \; = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \; key$ *and so is (* key *-* 1111*).*

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \; = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \; key$ *and so is (key -* 1111*).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \ key$ *and so is (* key - 1111*).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:*
   $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \ key \ = 37370$

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \; = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \; key$ *and so is (* key *-* 1111*).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:*
   $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \; key \; = 37370$
6. *Verifying:* $37370^2 \bmod \; key \; = 3310$

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \ key$ *and so is (* key *-* 1111*).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:* $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \ key \ = 37370$
6. *Verifying:* $37370^2 \bmod \ key \ = 3310$
7. *And the fourth square root is (key - 37370).*

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \ key$ *and so is (* key *- 1111).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:*
   $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \ key \ = 37370$
6. *Verifying:* $37370^2 \bmod \ key \ = 3310$
7. *And the fourth square root is (key - 37370).*

Discussion

So what can be done with this information? Can it be used to factor the key?

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \ key$ *and so is (* key *-* 1111*).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:*
   $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \ key \ = 37370$
6. *Verifying:* $37370^2 \bmod \ key \ = 3310$
7. *And the fourth square root is (key - 37370).*

Discussion

So what can be done with this information? Can it be used to factor the key?

Example

1. *Let* $p = 127, \quad q = 359, \quad key = 127 \cdot 359 = 45593.$
2. $1111^2 \bmod key \ = 3310$
3. *So* $1111 = \sqrt{3310} \bmod \ key$ *and so is (* key *- 1111).*
4. *The extended gcd gives us:* $147 \cdot 127 - 52 \cdot 359 = 1$
5. *So a third square root is:*
   $(147 \cdot 127 + 52 \cdot 359)1111 \bmod \ key \ = 37370$
6. *Verifying:* $37370^2 \bmod \ key \ = 3310$
7. *And the fourth square root is (key - 37370).*

Discussion

So what can be done with this information? Can it be used to factor the key?

Any other uses?

Comment

Finding $\sqrt{n} \mod pq$ *is as hard as factoring.*

Comment

Finding $\sqrt{n} \bmod pq$ *is as hard as factoring.*

Comment

Finding $\sqrt{n} \mod pq$ *is as hard as factoring.*

Indeed, assume you know how to calculate the four square roots of an integer $n \mod pq$*. This means that you have* $a^2 = b^2 \mod pq$ *or* $a^2 - b^2 = (a-b)(a+b) = c \cdot pq$*. Then with very high probability* $\gcd(a-b, pq)$ *or* $\gcd(a+b, pq)$ *will be* p *or* q*.*

Example

Consider the 74 digits key:

91449759565046891820618541051059950442886635729482
495300765336310642001663

Example

Consider the 74 digits key:

91449759565046891820618541051059950442886635729482
495300765336310642001663

Example

Consider the 74 digits key:

91449759565046891820618541051059950442886635729482 495300765336310642001663

Let $a = 91449759565046891820618541051059950442886635729482 495300765336309530890552$

and $b = 30411776568235771524836013708017059958 46323310698760664301089840386599710 3$

Example

Consider the 74 digits key:

91449759565046891820618541051059950442886635729482 495300765336310642001663

Let $a = 91449759565046891820618541051059950442886635729482495300765336309530890552$

and $b = 30411776568235771524836013708017059958463233106987606643010898403865997103$

$a^2 - b^2 \mod key = 0$

Example

Consider the 74 digits key:

91449759565046891820618541051059950442886635729482
495300765336310642001663

Let $a = 9144975956504689182061854105105995044288$
$6635729482495300765336309530890552$

and $b = 3041177656823577152483601370801705995 8$
$4632331069876066430108984038659971 03$

$a^2 - b^2 \bmod \; key \; = 0$

$gcd((a-b), key) = 2008341521442811032096543687424221 1$

$key = 20083415214428110320965436874242211 \cdot$
$45534964341796082033972201019765027517 33$

and the key has been factored.

Question

How difficult is finding two integers a, b such that $a^2 = b^2 \mod pq$?

Question

How difficult is finding two integers a, b such that $a^2 = b^2 \mod pq$?

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$, but still difficult.

Question

How difficult is finding two integers a, b such that $a^2 = b^2 \mod pq$?

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$, but still difficult.

Question

How difficult is finding two integers a, b such that $a^2 = b^2 \mod pq$?

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$, but still difficult.

The birthday paradox: how many randomly selected persons are needed so that the probability that two of them have the same birthdate is $> 50\%$?

Question

How difficult is finding two integers a, b *such that* $a^2 = b^2 \mod pq$*?*

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$*, but still difficult.*

The birthday paradox: how many randomly selected persons are needed so that the probability that two of them have the same birthdate is $> 50\%$*?*

The somewhat surprising answer is 23*.*

Question

How difficult is finding two integers a, b such that $a^2 = b^2 \mod pq$?

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$, but still difficult.

The birthday paradox: how many randomly selected persons are needed so that the probability that two of them have the same birthdate is $> 50\%$?

The somewhat surprising answer is 23.

How many integers we need to select randomly from $\{1, 2, \ldots, key - 1\}$ to find a, b such that the probability that $a^2 = b^2 \mod key = 0$ will be $> 50\%$?

Question

How difficult is finding two integers a, b *such that* $a^2 = b^2 \mod pq$*?*

Answer

Not as difficult as checking all primes less than $\sqrt{pq}$*, but still difficult.*

The birthday paradox: how many randomly selected persons are needed so that the probability that two of them have the same birthdate is $> 50\%$*?*

The somewhat surprising answer is 23*.*

How many integers we need to select randomly from $\{1, 2, \ldots, key - 1\}$ *to find* a, b *such that the probability that* $a^2 = b^2 \mod key = 0$ *will be* $> 50\%$*?*

About $\sqrt{key}$*. while this is still a huge number it points to the possibility that maybe some yet undiscovered idea may lead to a faster factoring computation.*

Example

Example

1. *Assume that your key is* $k = 10717279$.

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$
5. *And the key has been factored,*

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$
5. *And the key has been factored,*

Question

How do you find two numbres such that $a^2 = b^2 \mod k$*?*

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$
5. *And the key has been factored,*

Question

How do you find two numbres such that $a^2 = b^2 \mod k$*?*

Answer

Genrate two numbers simultaneously: $x_n = f^{(n)}(1)$ *and* x_{2n}.

Example

1. *Assume that your key is* $k = 10717279$.
2. *Let* $f(i) = i^2 + 1 \mod k$.
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$
5. *And the key has been factored,*

Question

How do you find two numbres such that $a^2 = b^2 \mod k$*?*

Answer

Genrate two numbers simultaneously: $x_n = f^{(n)}(1)$ *and* x_{2n}.

Example

1. *Assume that your key is* $k = 10717279$*.*
2. *Let* $f(i) = i^2 + 1 \mod k$*.*
3. *After less than* 1200 *iterations we found that* $3452^2 = 1095^2 \mod k$
4. $gcd(3452 - 1095, k) = 2357, \quad k = 2357 \cdot 4547$
5. *And the key has been factored,*

Question

How do you find two numbres such that $a^2 = b^2 \mod k$*?*

Answer

Genrate two numbers simultaneously: $x_n = f^{(n)}(1)$ *and* x_{2n}*.*

If for some integers j, n $x_n = x_{n+j}$ *then there is an integer* s *for which* $x_s = x_{2s}$*. This means that all we have to do is just track the pairs* $\{x_n, x_{2n}\}$*.*

A better password: Zero Knowledge Proof.

From the user point of view, the password system has changed little since its inception more than 70 years ago. The user selects a password, has to memorize it and uses it repeatedly. He risks the minor headache of forgetting it or the major problem of being stolen by various means.

A better password: Zero Knowledge Proof.

From the user point of view, the password system has changed little since its inception more than 70 years ago. The user selects a password, has to memorize it and uses it repeatedly. He risks the minor headache of forgetting it or the major problem of being stolen by various means.

The concept of *Zero Knowledge Proof* was introduced recently. The idea is to build a system by which I can prove to you that I know something while you will not be able to use it or learn anything you did not know before.

A better password: Zero Knowledge Proof.

From the user point of view, the password system has changed little since its inception more than 70 years ago. The user selects a password, has to memorize it and uses it repeatedly. He risks the minor headache of forgetting it or the major problem of being stolen by various means.

The concept of *Zero Knowledge Proof* was introduced recently. The idea is to build a system by which I can prove to you that I know something while you will not be able to use it or learn anything you did not know before.

Assume that you open a bank account. To create a password, you give the bank a "key", an integer $k = p \cdot q$ where $p,\ q$ are large prime numbers and $p, q \bmod 4 = 3$. You keep *p and q* secretely and securely. Everyone else may know or intercept your key.

To open a commnication, the bank selects a random integer r and calculates $r^2 \mod key$. The bank then sends you an integer $m = r^4 \mod key$.

To open a commnication, the bank selects a random integer r and calculates $r^2 \mod key$. The bank then sends you an integer $m = r^4 \mod key$.

While everyone knows the calculations involved, and may be able to intercept the message m, may know the key, they will not be able to calculate $\sqrt{m} \mod key$ unless they can factor the key.

To open a commnication, the bank selects a random integer r and calculates $r^2 \mod key$. The bank then sends you an integer $m = r^4 \mod key$.

While everyone knows the calculations involved, and may be able to intercept the message m, may know the key, they will not be able to calculate $\sqrt{m} \mod key$ unless they can factor the key.

You on the other hand, knowing p *and* q can calculate $\sqrt{m} \mod key$, but there are 4 disitnct square roots. Which one did the bank use? Furtheremore, if you send a different square root than the one used by the bank, someone at the bank will be able to factor your key.

Zero Knwledge Proofs

Herein lies the beauty of this system.

Herein lies the beauty of this system.
Becuase p *and* $q \mod 4 = 3$, -1 is not a quadratic residue mod p *or* q, only one of the four square roots of m has a square root mod *key* so you calculate the square root and send the bank its square, namely r^2.

Herein lies the beauty of this system.
Becuase $p \; and \; q \mod 4 = 3$, -1 is not a quadratic residue mod $p \; or \; q$, only one of the four square roots of m has a square root mod *key* so you calculate the square root and send the bank its square, namely r^2.

1. The bank receives r^2 which matches what he used to create m.

Zero Knwledge Proofs

Herein lies the beauty of this system.
Becuase $p \text{ and } q \mod 4 = 3$, -1 is not a quadratic residue mod p or q, only one of the four square roots of m has a square root mod *key* so you calculate the square root and send the bank its square, namely r^2.

1. The bank receives r^2 which matches what he used to create m.
2. The bank can now verify that you are communicating with the bank.

Zero Knwledge Proofs

Herein lies the beauty of this system.
Becuase $p \text{ and } q \mod 4 = 3$, -1 is not a quadratic residue mod p *or* q, only one of the four square roots of m has a square root mod *key* so you calculate the square root and send the bank its square, namely r^2.

1. The bank receives r^2 which matches what he used to create m.
2. The bank can now verify that you are communicating with the bank.
3. The bank did not get any knowledge he did not have before.

Zero Knwledge Proofs

Herein lies the beauty of this system.
Becuase p *and* $q \mod 4 = 3$, -1 is not a quadratic residue mod p *or* q, only one of the four square roots of m has a square root mod *key* so you calculate the square root and send the bank its square, namely r^2.

1. The bank receives r^2 which matches what he used to create m.
2. The bank can now verify that you are communicating with the bank.
3. The bank did not get any knowledge he did not have before.
4. For every communication a different m is used, so interecpting your response will not give any one any useful information.