Math 134: Cryptography

Lecture 8: More on RSA

Eoin Mackall

January 24, 2025

University of California, Santa Cruz

Last time

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

1. Bob picks beforehand two (large) prime numbers $p \neq q$ and computes their product $n = pq$.

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

1. Bob picks beforehand two (large) prime numbers $p \neq q$ and computes their product $n = pq$.
2. Bob chooses an integer e with $\gcd(e, \phi(n)) = 1$.

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

1. Bob picks beforehand two (large) prime numbers $p \neq q$ and computes their product $n = pq$.
2. Bob chooses an integer e with $\gcd(e, \phi(n)) = 1$.
3. Bob sends Alice the pair (n, e).

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

1. Bob picks beforehand two (large) prime numbers $p \neq q$ and computes their product $n = pq$.
2. Bob chooses an integer e with $\gcd(e, \phi(n)) = 1$.
3. Bob sends Alice the pair (n, e).
4. Alice will send her message in the form of an integer $m \in \mathbb{Z}$. If $m > n$, then Alice breaks $m = m_1 m_2 m_3 ...$ into blocks m_i of sizes less than n.

The RSA encryption algorithm

Alice wants to send a message to Bob. Bob has indicated that he wants to use RSA. What is the process for encryption?

1. Bob picks beforehand two (large) prime numbers $p \neq q$ and computes their product $n = pq$.
2. Bob chooses an integer e with $\gcd(e, \phi(n)) = 1$.
3. Bob sends Alice the pair (n, e).
4. Alice will send her message in the form of an integer $m \in \mathbb{Z}$. If $m > n$, then Alice breaks $m = m_1 m_2 m_3 \ldots$ into blocks m_i of sizes less than n.
5. For each block m_i, Alice computes the number $0 \leq r_i < n$ with $m_i^e \equiv r_i \pmod{n}$. She then sends Bob the numbers $r_1, r_2, r_3, \ldots$.

The RSA decryption algorithm

Bob has received a message from Alice. Bob had indicated that he wanted to use RSA for communication. What is the process for decryption?

The RSA decryption algorithm

Bob has received a message from Alice. Bob had indicated that he wanted to use RSA for communication. What is the process for decryption?

1. Prior to their communication, Bob had selected an integer d with $ed \equiv 1 \pmod{\phi(n)}$. Bob probably did this while computing $\gcd(e, \phi(n)) = 1$ (using, e.g. the Euclidean algorithm).

The RSA decryption algorithm

Bob has received a message from Alice. Bob had indicated that he wanted to use RSA for communication. What is the process for decryption?

1. Prior to their communication, Bob had selected an integer d with $ed \equiv 1 \pmod{\phi(n)}$. Bob probably did this while computing $\gcd(e, \phi(n)) = 1$ (using, e.g. the Euclidean algorithm).
2. Bob receives a sequence of integers $r_1, r_2, r_3, \ldots$ from Alice.

The RSA decryption algorithm

Bob has received a message from Alice. Bob had indicated that he wanted to use RSA for communication. What is the process for decryption?

1. Prior to their communication, Bob had selected an integer d with $ed \equiv 1 \pmod{\phi(n)}$. Bob probably did this while computing $\gcd(e, \phi(n)) = 1$ (using, e.g. the Euclidean algorithm).
2. Bob receives a sequence of integers $r_1, r_2, r_3, \ldots$ from Alice.
3. For each integer r_i, bob computes

$$r_i^d \equiv (m_i^e)^d \equiv m_i^{ed} \equiv m_i \pmod{n}.$$

The RSA decryption algorithm

Bob has received a message from Alice. Bob had indicated that he wanted to use RSA for communication. What is the process for decryption?

1. Prior to their communication, Bob had selected an integer d with $ed \equiv 1 \pmod{\phi(n)}$. Bob probably did this while computing $\gcd(e, \phi(n)) = 1$ (using, e.g. the Euclidean algorithm).
2. Bob receives a sequence of integers $r_1, r_2, r_3, \ldots$ from Alice.
3. For each integer r_i, bob computes

$$r_i^d \equiv (m_i^e)^d \equiv m_i^{ed} \equiv m_i \pmod{n}.$$

4. Bob combines these integers to obtain Alice's message $m = m_1 m_2 m_3 \ldots.$

Table of contents

Why RSA works

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

$$(m^e)^d \equiv m^{de} \pmod{n}$$

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

$$\begin{aligned}(m^e)^d &\equiv m^{de} \pmod{n} \\ &\equiv m^{k\phi(n)+1} \pmod{n}\end{aligned}$$

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

$$\begin{aligned}(m^e)^d &\equiv m^{de} \pmod{n} \\ &\equiv m^{k\phi(n)+1} \pmod{n} \\ &\equiv (m^{\phi(n)})^k \cdot m \pmod{n}\end{aligned}$$

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

$$\begin{aligned}
(m^e)^d &\equiv m^{de} \pmod{n} \\
&\equiv m^{k\phi(n)+1} \pmod{n} \\
&\equiv (m^{\phi(n)})^k \cdot m \pmod{n} \\
&\equiv (1)^k \cdot m \pmod{n}
\end{aligned}$$

Messages that are coprime to n

Alice wants to send a message to Bob. Bob suggests using RSA to communicate. Bob sends Alice the public encryption key (n, e) and keeps private a decryption key d.

Suppose that Alice's message m is coprime to n, i.e. $\gcd(m, n) = 1$.

Then since $de \equiv 1 \pmod{\phi(n)}$, there is a $k \in \mathbb{Z}$ with $de = k\phi(n) + 1$. We can compute:

$$\begin{aligned}
(m^e)^d &\equiv m^{de} \pmod{n} \\
&\equiv m^{k\phi(n)+1} \pmod{n} \\
&\equiv (m^{\phi(n)})^k \cdot m \pmod{n} \\
&\equiv (1)^k \cdot m \pmod{n} \\
&\equiv m \pmod{n}.
\end{aligned}$$

Messages that are coprime to n

What if $\gcd(m, n) \neq 1$?

Messages that are coprime to n

What if $\gcd(m, n) \neq 1$?

If $\gcd(m, n) \neq 1$ then, since $n = pq$ for primes p, q we must have either $p \mid m$ or $q \mid m$.

Messages that are coprime to n

What if $\gcd(m, n) \neq 1$?

If $\gcd(m, n) \neq 1$ then, since $n = pq$ for primes p, q we must have either $p \mid m$ or $q \mid m$.

Suppose that $p, q \approx 10^{150}$ so that $n \approx 10^{300}$. Then there are $n/p = q$ many numbers between p and n divisible by p. Similarly there are $n/q = p$ many numbers between q and n divisible by q.

Messages that are coprime to n

What if $\gcd(m, n) \neq 1$?

If $\gcd(m, n) \neq 1$ then, since $n = pq$ for primes p, q we must have either $p \mid m$ or $q \mid m$.

Suppose that $p, q \approx 10^{150}$ so that $n \approx 10^{300}$. Then there are $n/p = q$ many numbers between p and n divisible by p. Similarly there are $n/q = p$ many numbers between q and n divisible by q.

This means there are no more than $p + q \approx 2 \cdot 10^{150}$ numbers divisible by one of p or q. Assuming that m appears in $[0, n-1]$ randomly and uniformly, the probability that $\gcd(m, n) \neq 1$ is then

$$\mathbb{P}(\gcd(m, n) \neq 1) \approx (2 \cdot 10^{150})/(10^{300}) \approx 2 \cdot 10^{-150}.$$

Messages that are coprime to n

What if $\gcd(m,n) \neq 1$?

If $\gcd(m,n) \neq 1$ then, since $n = pq$ for primes p, q we must have either $p \mid m$ or $q \mid m$.

Suppose that $p, q \approx 10^{150}$ so that $n \approx 10^{300}$. Then there are $n/p = q$ many numbers between p and n divisible by p. Similarly there are $n/q = p$ many numbers between q and n divisible by q.

This means there are no more than $p + q \approx 2 \cdot 10^{150}$ numbers divisible by one of p or q. Assuming that m appears in $[0, n-1]$ randomly and uniformly, the probability that $\gcd(m,n) \neq 1$ is then

$$\mathbb{P}(\gcd(m,n) \neq 1) \approx (2 \cdot 10^{150})/(10^{300}) \approx 2 \cdot 10^{-150}.$$

Still, what if $\gcd(m,n) \neq 1$?

The Chinese Remainder Theorem

Let $a, b \in \mathbb{Z}$ be two integers with $\gcd(a, b) = 1$.

Let $a, b \in \mathbb{Z}$ be two integers with $\gcd(a, b) = 1$.

Theorem (The Chinese Remainder Theorem)

Let $r, s \in \mathbb{Z}$ be arbitrary, a and b as above. Then there exists a solution $x \in \mathbb{Z}$ to the system of equations

$$x \equiv r \pmod{a}$$
$$x \equiv s \pmod{b}.$$

An integer $x' \in \mathbb{Z}$ solves the above system if and only if $x \equiv x' \pmod{ab}$. In particular, there is a unique solution x to the above system with $0 \leq x < ab$.

The Chinese Remainder Theorem

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Proof.

Since $\gcd(a,b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Let $x = r(bn) + s(am)$.

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Let $x = r(bn) + s(am)$. Then

$$x \equiv r(bn) \equiv r \pmod{a}$$

$\square$

The Chinese Remainder Theorem

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Let $x = r(bn) + s(am)$. Then

$$x \equiv r(bn) \equiv r \pmod{a}$$
$$x \equiv s(am) \equiv s \pmod{b}.$$

$\square$

The Chinese Remainder Theorem

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Let $x = r(bn) + s(am)$. Then

$$x \equiv r(bn) \equiv r \pmod{a}$$
$$x \equiv s(am) \equiv s \pmod{b}.$$

If x' is another solution, then $a \mid (x - x')$ and $b \mid (x - x')$ so $ab \mid (x - x')$ since $\gcd(a, b) = 1$. $\square$

The Chinese Remainder Theorem

Proof.

Since $\gcd(a, b) = 1$ we can find integers $m, n \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Note

$$am \equiv 1 \pmod{b} \quad \text{and} \quad bn \equiv 1 \pmod{a}.$$

Let $x = r(bn) + s(am)$. Then

$$x \equiv r(bn) \equiv r \pmod{a}$$
$$x \equiv s(am) \equiv s \pmod{b}.$$

If x' is another solution, then $a \mid (x - x')$ and $b \mid (x - x')$ so $ab \mid (x - x')$ since $\gcd(a, b) = 1$. The converse is easier. $\square$

Example

Let's solve the system of equations

$$x \equiv 6 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

for the unique integer $x \in \mathbb{Z}$ with $0 \leq x < 77$.

The Chinese Remainder Theorem

Example

Let's solve the system of equations

$$x \equiv 6 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

for the unique integer $x \in \mathbb{Z}$ with $0 \leq x < 77$.

Note that if $x \equiv 6 \pmod{7}$ then $x - 6 = 7k$ for some $k \in \mathbb{Z}$.

Example

Let's solve the system of equations

$$x \equiv 6 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

for the unique integer $x \in \mathbb{Z}$ with $0 \leq x < 77$.

Note that if $x \equiv 6 \pmod{7}$ then $x - 6 = 7k$ for some $k \in \mathbb{Z}$. Hence $6 + 7k \equiv 3 \pmod{11}$ so that

$$7k \equiv 3 - 6 \equiv -3 \equiv 8 \pmod{11}.$$

Example

Let's solve the system of equations

$$x \equiv 6 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

for the unique integer $x \in \mathbb{Z}$ with $0 \leq x < 77$.

Note that if $x \equiv 6 \pmod{7}$ then $x - 6 = 7k$ for some $k \in \mathbb{Z}$. Hence $6 + 7k \equiv 3 \pmod{11}$ so that

$$7k \equiv 3 - 6 \equiv -3 \equiv 8 \pmod{11}.$$

Since $7 \equiv -4 \pmod{11}$ and $(-3) \cdot (-4) \equiv 1 \pmod{11}$ we have

$$k \equiv (-3) \cdot 8 \equiv 9 \pmod{11}.$$

Example

Let's solve the system of equations

$$x \equiv 6 \pmod{7}$$
$$x \equiv 3 \pmod{11}$$

for the unique integer $x \in \mathbb{Z}$ with $0 \leq x < 77$.

Note that if $x \equiv 6 \pmod{7}$ then $x - 6 = 7k$ for some $k \in \mathbb{Z}$. Hence $6 + 7k \equiv 3 \pmod{11}$ so that

$$7k \equiv 3 - 6 \equiv -3 \equiv 8 \pmod{11}.$$

Since $7 \equiv -4 \pmod{11}$ and $(-3) \cdot (-4) \equiv 1 \pmod{11}$ we have

$$k \equiv (-3) \cdot 8 \equiv 9 \pmod{11}.$$

Plugging this in gives $x = 7(9) + 6 = 69$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$.

Case I

If $\gcd(m, n) = p$ then $m \equiv 0 \pmod{p}$. Since $q \nmid m$, we have that $m \equiv a \not\equiv 0 \pmod{q}$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$.

Case I

If $\gcd(m, n) = p$ then $m \equiv 0 \pmod{p}$. Since $q \nmid m$, we have that $m \equiv a \not\equiv 0 \pmod{q}$.

Then we find

$$\begin{aligned} m^e &\equiv 0 \pmod{p} \\ m^e &\equiv a^e \pmod{q} \end{aligned}$$

so that

$$\begin{aligned} (m^e)^d &\equiv 0 \pmod{p} \\ (m^e)^d &\equiv a^{ed} \pmod{q}. \end{aligned}$$

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case I

If $\gcd(m, n) = p$ then $m \equiv 0 \pmod{p}$. Since $q \nmid m$, we have that $m \equiv a \not\equiv 0 \pmod{q}$.

$$\begin{aligned} (m^e)^d &\equiv 0 \pmod{p} \\ (m^e)^d &\equiv a^{ed} \pmod{q}. \end{aligned}$$

Since $ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$ we find

$$\begin{aligned} m^{ed} &\equiv 0 \pmod{p} \\ m^{ed} &\equiv a^{ed} \equiv a^{1+k(p-1)(q-1)} \equiv a \cdot (a^{q-1})^{k(p-1)} \equiv a \pmod{q} \end{aligned}$$

by Fermat's little theorem.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case I

If $\gcd(m, n) = p$ then $m \equiv 0 \pmod{p}$. Since $q \nmid m$, we have that $m \equiv a \not\equiv 0 \pmod{q}$.

Since $ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$ we find

$$
\begin{aligned}
m^{ed} &\equiv 0 \pmod{p} \\
m^{ed} &\equiv a^{ed} \equiv a^{1+k(p-1)(q-1)} \equiv a \cdot (a^{q-1})^{k(p-1)} \equiv a \pmod{q}
\end{aligned}
$$

by Fermat's little theorem.

Now the Chinese Remainder theorem implies that if $0 < m < n$ then $m^{ed} \equiv m \pmod{n}$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case II

If $\gcd(m, n) = q$,

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case II

If $\gcd(m, n) = q$, then we proceed in the same way as before.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case II

If $\gcd(m, n) = q$, then we proceed in the same way as before.

Case III

If $\gcd(m, n) = n$,

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case II

If $\gcd(m, n) = q$, then we proceed in the same way as before.

Case III

If $\gcd(m, n) = n$, then $m = 0$ and $m^r \equiv m \pmod{n}$ for all $r \geq 1$.

Messages that are not coprime to n

Suppose that $n = pq$ for primes p, q. Let $e \in \mathbb{Z}$ be an integer with $\gcd(e, \phi(n)) = 1$ and $d \in \mathbb{Z}$ be such that $de \equiv 1 \pmod{\phi(n)}$.

Let $m \in \mathbb{Z}$ be an integer such that $\gcd(m, n) \neq 1$

Case II

If $\gcd(m, n) = q$, then we proceed in the same way as before.

Case III

If $\gcd(m, n) = n$, then $m = 0$ and $m^r \equiv m \pmod{n}$ for all $r \geq 1$.

Thus, for every integer message m, we may recover m exactly after RSA encryption and decryption.

Basis for RSA security

Factoring

The security of RSA is dependent on an adversary being unable to find the secret key d that Bob uses for decryption.

Factoring

The security of RSA is dependent on an adversary being unable to find the secret key d that Bob uses for decryption.

Claim

This security is closely related to the problem of factoring integers.

Factoring

The security of RSA is dependent on an adversary being unable to find the secret key d that Bob uses for decryption.

Claim

This security is closely related to the problem of factoring integers.

Justification

Suppose that Eve can factor n and recover the primes p, q that Bob uses in his RSA scheme.

Factoring

The security of RSA is dependent on an adversary being unable to find the secret key d that Bob uses for decryption.

Claim

This security is closely related to the problem of factoring integers.

Justification

Suppose that Eve can factor n and recover the primes p, q that Bob uses in his RSA scheme.

Then Eve can calculate $\phi(n) = (p-1)(q-1)$ and, since everyone knows the value of e, she may (efficiently) find an integer $d \in \mathbb{Z}$ with $ed \equiv 1 \pmod{\phi(n)}$ using the Euclidean algorithm.

Factoring

The security of RSA is dependent on an adversary being unable to find the secret key d that Bob uses for decryption.

Claim

This security is closely related to the problem of factoring integers.

Justification

Suppose that Eve can factor n and recover the primes p, q that Bob uses in his RSA scheme.

Then Eve can calculate $\phi(n) = (p-1)(q-1)$ and, since everyone knows the value of e, she may (efficiently) find an integer $d \in \mathbb{Z}$ with $ed \equiv 1 \pmod{\phi(n)}$ using the Euclidean algorithm.

We will come back to the other direction momentarily.

Factoring

Clearly if Eve knows $\phi(n)$, then Eve may break Bob's RSA encryption scheme. Maybe it is easier to find $\phi(n)$ than to factor n?

Factoring

Clearly if Eve knows $\phi(n)$, then Eve may break Bob's RSA encryption scheme. Maybe it is easier to find $\phi(n)$ than to factor n?

Claim

If Eve knows $\phi(n)$, then Eve can factor n.

Factoring

Clearly if Eve knows $\phi(n)$, then Eve may break Bob's RSA encryption scheme. Maybe it is easier to find $\phi(n)$ than to factor n?

Claim

If Eve knows $\phi(n)$, then Eve can factor n.

Justification

Since $n = pq$, we know that $\phi(n) = (p-1)(q-1) = pq - p - q + 1$.

Factoring

Clearly if Eve knows $\phi(n)$, then Eve may break Bob's RSA encryption scheme. Maybe it is easier to find $\phi(n)$ than to factor n?

Claim

If Eve knows $\phi(n)$, then Eve can factor n.

Justification

Since $n = pq$, we know that $\phi(n) = (p-1)(q-1) = pq - p - q + 1$.

Hence if Eve knows n and $\phi(n)$, Eve may quickly find

$$n - \phi(n) + 1 = pq - (pq - p - q + 1) + 1 = p + q.$$

Factoring

Clearly if Eve knows $\phi(n)$, then Eve may break Bob's RSA encryption scheme. Maybe it is easier to find $\phi(n)$ than to factor n?

Claim

If Eve knows $\phi(n)$, then Eve can factor n.

Justification

Since $n = pq$, we know that $\phi(n) = (p-1)(q-1) = pq - p - q + 1$.

Hence if Eve knows n and $\phi(n)$, Eve may quickly find

$$n - \phi(n) + 1 = pq - (pq - p - q + 1) + 1 = p + q.$$

But then

$$X^2 - (n - \phi(n) + 1)X + n = X^2 - (p+q)X + pq = (X-p)(X-q)$$

and the quadratic formula can be used to find p, q. So Eve can factor n.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

Remember that $de \equiv 1 \pmod{(p-1)(q-1)}$. So there exists $k \in \mathbb{Z}$ with $de = 1 + k(p-1)(q-1)$.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

Remember that $de \equiv 1 \pmod{(p-1)(q-1)}$. So there exists $k \in \mathbb{Z}$ with $de = 1 + k(p-1)(q-1)$.

Since d (or an equivalent number) has the property that $0 < d < (p-1)(q-1)$ we have

$$(p-1)(q-1)k < de < (p-1)(q-1)e.$$

This implies $k < e$.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

Now with $de = 1 + k(p-1)(q-1)$ we have

$$k = \frac{de-1}{(p-1)(q-1)} > \frac{de-1}{n} = \frac{(p-1)(q-1)k}{n} = \frac{(pq-p-q+1)k}{n}$$

$$= k - \frac{(p+q-1)k}{n}.$$

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

Now with $de = 1 + k(p-1)(q-1)$ we have

$$k = \frac{de-1}{(p-1)(q-1)} > \frac{de-1}{n} = \frac{(p-1)(q-1)k}{n} = \frac{(pq-p-q+1)k}{n}$$

$$= k - \frac{(p+q-1)k}{n}.$$

If p, q are large primes, then usually n is much larger. Since $k < e$, if we know that e is sufficiently small, then $0 \leq (p+q-1)k/n << 1$.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

So if e is sufficiently small, we can compute $k = \lceil (de - 1)/n \rceil$.

Factoring

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

So if e is sufficiently small, we can compute $k = \lceil (de - 1)/n \rceil$.

Now we can solve $de - 1 = \phi(n)k$ to find $\phi(n)$.

It would be desirable if, supposing that Eve knows d, this would imply that Eve could factor n.

Here is some evidence to that effect.

Claim

If e is sufficiently small, and if Eve knows d, then Eve can factor n.

Justification

So if e is sufficiently small, we can compute $k = \lceil (de - 1)/n \rceil$.

Now we can solve $de - 1 = \phi(n)k$ to find $\phi(n)$.

Knowing $\phi(n)$, we can factor n.