Remainders of Security: from Modular Arithmetic to Cryptography

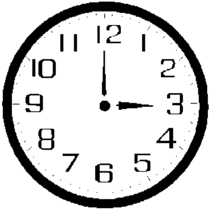
Dr Julia Goedecke

Newnham College

6 July 2017, Open Day

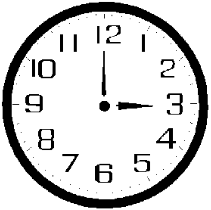
Remainders

- If it is 3 o'clock now, what time is it in 10 hours?
- If it is Thursday now, what day is it in 9 days?
- If it is summer now, what season will it be in 100 seasons?
- If it is midday now, will it be light or dark in 539 hours?



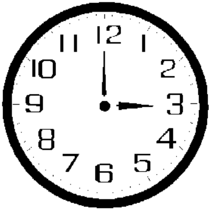
Remainders

- If it is 3 o'clock now, what time is it in 10 hours?
- If it is Thursday now, what day is it in 9 days?
- If it is summer now, what season will it be in 100 seasons?
- If it is midday now, will it be light or dark in 539 hours?



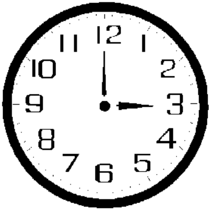
Remainders

- If it is 3 o'clock now, what time is it in 10 hours?
- If it is Thursday now, what day is it in 9 days?
- If it is summer now, what season will it be in 100 seasons?
- If it is midday now, will it be light or dark in 539 hours?



Remainders

- If it is 3 o'clock now, what time is it in 10 hours?
- If it is Thursday now, what day is it in 9 days?
- If it is summer now, what season will it be in 100 seasons?
- If it is midday now, will it be light or dark in 539 hours?



Calculating with remainders

Writing the above answers mathematically

- $3 + 10 \equiv 1 \pmod{12}$ So 1 o'clock.
- $4 + 9 \equiv 6 \pmod{7}$ So Saturday.
- $2 + 100 \equiv 2 \pmod{4}$ So summer again.
- $12 + 539 \equiv 12 + 480 + 59 \equiv 12 + 11 \equiv 23 \pmod{24}$
  So it will be 23h, or 11pm, so dark.

Modular Arithmetic

Formally

For whole numbers x, y and n we write

$$x \equiv y \pmod{n} \iff (x-y) = kn \quad \text{for some whole number } k.$$

Two numbers are congruent modulo n exactly when their difference is divisible by n.

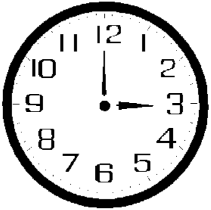
Modular Arithmetic

Formally

For whole numbers x, y and n we write

$$x \equiv y \pmod{n} \iff (x - y) = kn \quad \text{for some whole number } k.$$

Two numbers are congruent modulo n exactly when their difference is divisible by n.



Multiplication mod n

Multiplication modulo 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2			
3	0	3			
4	0	4			

Multiplication modulo 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2				
3	0	3				
4	0	4				
5	0	5				

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2				
3	0	3				
4	0	4				
5	0	5				

Multiplication mod n

Multiplication modulo 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2				
3	0	3				
4	0	4				
5	0	5				

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2				
3	0	3				
4	0	4				
5	0	5				

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication mod n

Multiplication modulo 5

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplication mod n

Multiplication modulo 5

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication modulo 6

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Inverse

We say y is an inverse of x mod n if $xy \equiv 1 \pmod{n}$.

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Airlifted in: Bezout's Identity

If a, b coprime integers, then there are integers x, y such that

$$ax + by = 1.$$

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Airlifted in: Bezout's Identity

If a, b coprime integers, then there are integers x, y such that

$$ax + by = 1.$$

Proof

p prime, $a \not\equiv 0 \pmod p \Rightarrow p, a$ coprime.

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Airlifted in: Bezout's Identity

If a, b coprime integers, then there are integers x, y such that

$$ax + by = 1.$$

Proof

p prime, $a \not\equiv 0 \pmod{p} \Rightarrow p, a$ coprime.

So by Bezout, we have $px + ay = 1$ for some x, y.

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Airlifted in: Bezout's Identity

If a, b coprime integers, then there are integers x, y such that

$$ax + by = 1.$$

Proof

p prime, $a \not\equiv 0 \pmod{p} \Rightarrow p, a$ coprime.

So by Bezout, we have $px + ay = 1$ for some x, y.

$\Rightarrow ay \equiv 1 \pmod{p}$.

Inverses for primes

Lemma

If p is prime, then every non-zero number mod p has an inverse mod p.

Airlifted in: Bezout's Identity

If a, b coprime integers, then there are integers x, y such that

$$ax + by = 1.$$

Proof

p prime, $a \not\equiv 0 \pmod{p} \Rightarrow p, a$ coprime.

So by Bezout, we have $px + ay = 1$ for some x, y.

$\Rightarrow ay \equiv 1 \pmod{p}$.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$?

Calculations and thoughts

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$?

Calculations and thoughts

a contains not a single factor of n.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$?

Calculations and thoughts

a contains not a single factor of n.

All the numbers $1, \ldots, (n-1)$ are less than n.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$?

Calculations and thoughts

a contains not a single factor of n.

All the numbers $1, \ldots, (n-1)$ are less than n.

So n can't be formed as a factor of any of those numbers!

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.

Calculations and thoughts

a contains not a single factor of n.

All the numbers $1, \ldots, (n-1)$ are less than n.

So n can't be formed as a factor of any of those numbers!

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \dots, (n-1)a$ mod n.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n?

Calculations and thoughts

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \dots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n?

Calculations and thoughts

Suppose $ka \equiv la \pmod{n}$, with $l < k$.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n?

Calculations and thoughts

Suppose $ka \equiv la \pmod{n}$, with $l < k$.

That means $ka - la = (k-l)a$ is a multiple of n.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a$ mod n.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n?

Calculations and thoughts

Suppose $ka \equiv la \pmod{n}$, with $l < k$.

That means $ka - la = (k - l)a$ is a multiple of n.

But we have explained that this can't happen if $k - l < n$ which it is.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \dots, (n-1)a$ mod n.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n? No! They must all be different.

Calculations and thoughts

Suppose $ka \equiv la \pmod{n}$, with $l < k$.

That means $ka - la = (k - l)a$ is a multiple of n.

But we have explained that this can't happen if $k - l < n$ which it is.

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n? No! They must all be different.
- Which numbers mod n can they be?

Calculations and thoughts

A little exercise

For n and a coprime, consider the numbers $a, 2a, 3a, \ldots, (n-1)a \bmod n$.

- Is it possible that any of these is $0 \pmod{n}$? No! They are all non-zero mod n.
- Can any two be the same mod n? No! They must all be different.
- Which numbers mod n can they be? Since all different, they are $1, 2, \ldots, (n-1)$ in some order.

Calculations and thoughts

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.
- Or take all factors of a to the front.

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.
- Or take all factors of a to the front.
- So $1 \cdot 2 \cdots (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$.

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.
- Or take all factors of a to the front.
- So $1 \cdot 2 \cdots (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$.
- But each of $1, 2, \ldots, p-1$ has an inverse mod p!

Fermat's Little Theorem

Theorem (Little Fermat)

If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.
- Or take all factors of a to the front.
- So $1 \cdot 2 \cdots (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$.
- But each of $1, 2, \ldots, p-1$ has an inverse mod p!
- Multiply both sides by all these inverses, to get:

Fermat's Little Theorem

Theorem (Little Fermat)

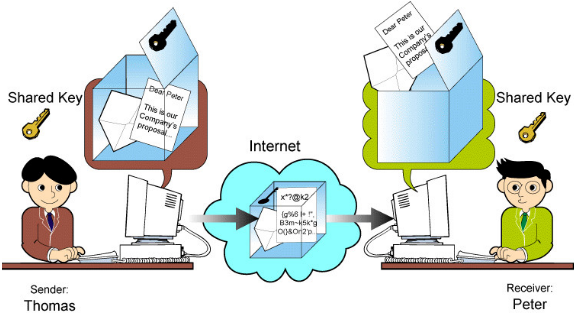
If p prime and a not a multiple of p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

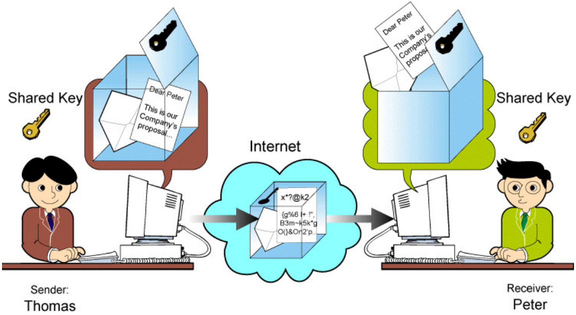
Proof

- Consider product of $a, 2a, 3a, \ldots, (p-1)a$ in two ways:
- Same numbers as $1, 2, \ldots, (p-1)$, so have same product.
- Or take all factors of a to the front.
- So $1 \cdot 2 \cdots (p-1) \equiv a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$.
- But each of $1, 2, \ldots, p-1$ has an inverse mod p!
- Multiply both sides by all these inverses, to get:
- $1 \equiv a^{p-1} \pmod{p}$.

Cryptography



Cryptography



- write secret messages
- store data securely
- secure internet payment
- secret radio transmission in war
- ...

Caesar Cipher

How does it work?

- Our friend moves to Australia, we want to send them a secret letter.
- We can use different “shifts”: our key.
- We write secret sentence using key.
- How will recipient know key?

Link to modular arithmetic

What's it got to do with what we did before?

- Substitute numbers for the letters: $A = 1$, $B = 2$, $C = 3$ etc. up to $Z = 26$

Link to modular arithmetic

What's it got to do with what we did before?

- Substitute numbers for the letters: $A = 1$, $B = 2$, $C = 3$ etc. up to $Z = 26$
- Pick a number as your key: we'll call it φ.

Link to modular arithmetic

What's it got to do with what we did before?

- Substitute numbers for the letters: $A = 1$, $B = 2$, $C = 3$ etc. up to $Z = 26$
- Pick a number as your key: we'll call it φ.
- For each letter (now a number α) of your message, calculate

$$\beta \equiv \alpha + \varphi \pmod{26}.$$

Link to modular arithmetic

What's it got to do with what we did before?

- Substitute numbers for the letters: $A = 1$, $B = 2$, $C = 3$ etc. up to $Z = 26$
- Pick a number as your key: we'll call it φ.
- For each letter (now a number α) of your message, calculate

$$\beta \equiv \alpha + \varphi \pmod{26}.$$

- Transmit β (a string of such βs, one each for each letter of your message).

Link to modular arithmetic

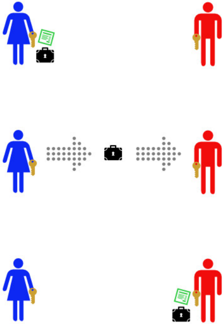
What's it got to do with what we did before?

- Substitute numbers for the letters: $A = 1$, $B = 2$, $C = 3$ etc. up to $Z = 26$
- Pick a number as your key: we'll call it φ.
- For each letter (now a number α) of your message, calculate
$$\beta \equiv \alpha + \varphi \pmod{26}.$$
- Transmit β (a string of such βs, one each for each letter of your message).
- To decipher, recipient needs to calculate
$$\beta - \varphi \pmod{26}$$
to get your original message α back.

Symmetric Key Cryptography

Problems

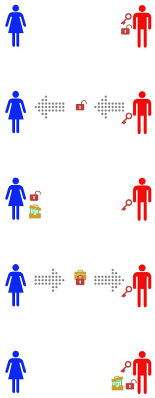
- Alice and Bob want secret communication.
- Both need same key.
- Problem: safe key exchange.
- Doesn't work for internet shopping.



Public Key Cryptography

Padlock metaphor

- Bob has padlock and matching key.
- Alice can get open padlock from internet.
- Alice padlocks the message for Bob.
- Message now safe to send.
- Only Bob has the key to open it.



RSA Algorithm

How it works

- Take two large primes p and q.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.
- Choose public key $e \leq \varphi$ which has no factors in common with φ.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.
- Choose public key $e \leq \varphi$ which has no factors in common with φ.
- Calculate private key d which satisfies $de \equiv 1 \pmod{\varphi}$.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.
- Choose public key $e \leq \varphi$ which has no factors in common with φ.
- Calculate private key d which satisfies $de \equiv 1 \pmod{\varphi}$.
- Throw away p, q and φ.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.
- Choose public key $e \leq \varphi$ which has no factors in common with φ.
- Calculate private key d which satisfies $de \equiv 1 \pmod{\varphi}$.
- Throw away p, q and φ.
- Encrypt message x as $y \equiv x^e \pmod{n}$.

RSA Algorithm

How it works

- Take two large primes p and q.
- Calculate $n = pq$ and $\varphi = (p-1)(q-1)$.
- Choose public key $e \leq \varphi$ which has no factors in common with φ.
- Calculate private key d which satisfies $de \equiv 1 \pmod{\varphi}$.
- Throw away p, q and φ.
- Encrypt message x as $y \equiv x^e \pmod{n}$.
- Decrypt ciphertext y as $x \equiv y^d \pmod{n}$.

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Proof

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1}$$

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)}$$

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)}.$$

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)}.$$

But Little Fermat $\Rightarrow$ $x^{(p-1)} \equiv 1 \pmod{p}$ as long as $x \not\equiv 0 \pmod{p}$.

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)}.$$

But Little Fermat $\Rightarrow x^{(p-1)} \equiv 1 \pmod{p}$ as long as $x \not\equiv 0 \pmod{p}$.

So $x^{ed} = x \cdot (x^{(p-1)})^{k(q-1)}$

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)}.$$

But Little Fermat $\Rightarrow$ $x^{(p-1)} \equiv 1 \pmod{p}$ as long as $x \not\equiv 0 \pmod{p}$.

So $x^{ed} = x \cdot (x^{(p-1)})^{k(q-1)} \equiv x \cdot 1^{k(q-1)} = x \pmod{p}$.

RSA Algorithm

Does it really work?

Can we get the correct message back? Is $(x^e)^d \equiv x \pmod{n}$?

Airlifted in

Enough to show $(x^e)^d \equiv x \pmod{p}$ and $(x^e)^d \equiv x \pmod{q}$.

Proof

$$x^{ed} = x^{k\varphi+1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)}.$$

But Little Fermat $\Rightarrow x^{(p-1)} \equiv 1 \pmod{p}$ as long as $x \not\equiv 0 \pmod{p}$.

So $x^{ed} = x \cdot (x^{(p-1)})^{k(q-1)} \equiv x \cdot 1^{k(q-1)} = x \pmod{p}$.

Hurray!

RSA: Why is it safe?

Multiplying vs. Factorising

- Calculate $23 \cdot 37$.

RSA: Why is it safe?

Multiplying vs. Factorising

- Calculate $23 \cdot 37$.
- Find the factors of 943.

RSA: Why is it safe?

Multiplying vs. Factorising

- Calculate $23 \cdot 37$.
- Find the factors of 943.
- Which was faster/easier?

RSA: Why is it safe?

Multiplying vs. Factorising

- Calculate $23 \cdot 37$.
- Find the factors of 943.
- Which was faster/easier?
- To decipher, need to know d, for which we need φ, for which we need p and q: hard to get.

I hope you had some fun!