MAS114: Lecture 18

James Cranch

http://cranch.staff.shef.ac.uk/mas114/

2017–2018

Cryptography

Cryptography

In this section, we'll show off a major modern application of all the ideas above.

Cryptography

In this section, we'll show off a major modern application of all the ideas above. The aim is to talk about (one small but key part of) modern cryptography.

Cryptography

In this section, we'll show off a major modern application of all the ideas above. The aim is to talk about (one small but key part of) modern cryptography.

Cryptography is the study of how to send messages in a form which cannot be read except by the intended recipients.

Cryptography

In this section, we'll show off a major modern application of all the ideas above. The aim is to talk about (one small but key part of) modern cryptography.

Cryptography is the study of how to send messages in a form which cannot be read except by the intended recipients. To *encrypt* the messages is to put them in a form which cannot be read easily;

Cryptography

In this section, we'll show off a major modern application of all the ideas above. The aim is to talk about (one small but key part of) modern cryptography.

Cryptography is the study of how to send messages in a form which cannot be read except by the intended recipients. To *encrypt* the messages is to put them in a form which cannot be read easily; to *decrypt* the messages is to take such messages and recover them in readable form.

Dramatis personae

Dramatis personae

The literature of cryptography usually talks about three people:

Dramatis personae

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,

Dramatis personae

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,
- **Bob** who wishes to receive a private message from Alice, and

Dramatis personae

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,
- **Bob** who wishes to receive a private message from Alice, and
- **Eve** who wishes to find out what Alice is telling Bob.

Dramatis personae

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,
- **Bob** who wishes to receive a private message from Alice, and
- **Eve** who wishes to find out what Alice is telling Bob.

Alice and Bob are of course named so as to start with the letters A and B respectively.

Dramatis personae

The literature of cryptography usually talks about three people:

- **Alice** who wishes to send a private message to Bob,
- **Bob** who wishes to receive a private message from Alice, and
- **Eve** who wishes to find out what Alice is telling Bob.

Alice and Bob are of course named so as to start with the letters A and B respectively. Eve is so named because she is an *eavesdropper*, or perhaps because she is *evil*.

Old-time cryptography

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message.

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already!

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already! For example, you could substitute the letters of the alphabet according to some agreed system: then the key would describe that system and would be a list of facts like $A \mapsto Q$, $B \mapsto J$, etc.

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already! For example, you could substitute the letters of the alphabet according to some agreed system: then the key would describe that system and would be a list of facts like $A \mapsto Q$, $B \mapsto J$, etc.

The big disadvantage with that is that Alice and Bob have to exchange the key somehow at the beginning:

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already! For example, you could substitute the letters of the alphabet according to some agreed system: then the key would describe that system and would be a list of facts like $A \mapsto Q$, $B \mapsto J$, etc.

The big disadvantage with that is that Alice and Bob have to exchange the key somehow at the beginning: if Eve can spy on that conversation, she has the key and can decrypt Alice's message just as easily as Bob can.

Old-time cryptography

In the olden days, Alice and Bob would have come up with some kind of system depending on a shared secret *key* with which you could encrypt and decrypt a message. Perhaps you've seen many of these techniques already! For example, you could substitute the letters of the alphabet according to some agreed system: then the key would describe that system and would be a list of facts like $A \mapsto Q$, $B \mapsto J$, etc.

The big disadvantage with that is that Alice and Bob have to exchange the key somehow at the beginning: if Eve can spy on that conversation, she has the key and can decrypt Alice's message just as easily as Bob can.

The problem with this old-time approach is that the same secret is used to encrypt and decrypt the message, so needs exchanging.

Public-key cryptography

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.
3. Bob takes the key which tells you how to encrypt messages, the *public key*, and shares it with everyone who wants it, with no secrecy whatsoever. In particular, he sends Alice a postcard telling her his public key. Of course Eve finds it out quickly, but Bob doesn't care.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.
3. Bob takes the key which tells you how to encrypt messages, the *public key*, and shares it with everyone who wants it, with no secrecy whatsoever. In particular, he sends Alice a postcard telling her his public key. Of course Eve finds it out quickly, but Bob doesn't care.
4. Alice uses Bob's public key to encrypt a message for Bob.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.
3. Bob takes the key which tells you how to encrypt messages, the *public key*, and shares it with everyone who wants it, with no secrecy whatsoever. In particular, he sends Alice a postcard telling her his public key. Of course Eve finds it out quickly, but Bob doesn't care.
4. Alice uses Bob's public key to encrypt a message for Bob.
5. Alice sends Bob the encrypted message.

Public-key cryptography

Suppose instead there was a type of encryption with a key for encryption and another key for decryption, such that, even if you know exactly how to encrypt a message, it is very hard indeed to work out how to decrypt it.

That suggests the following plan:

1. Bob comes up with a system of encrypting and decrypting of that sort.
2. Bob takes the key which tells you how to decrypt messages, the *private key*, and keeps it to himself, never telling anyone.
3. Bob takes the key which tells you how to encrypt messages, the *public key*, and shares it with everyone who wants it, with no secrecy whatsoever. In particular, he sends Alice a postcard telling her his public key. Of course Eve finds it out quickly, but Bob doesn't care.
4. Alice uses Bob's public key to encrypt a message for Bob.
5. Alice sends Bob the encrypted message.
6. Bob uses his private key to decrypt it, and read Alice's message.

The details

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s.

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman.

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years).

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years). RSA is still in very widespread use on the internet.

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years). RSA is still in very widespread use on the internet.

The secret of RSA is to work modulo pq, where p and q are (different) primes.

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years). RSA is still in very widespread use on the internet.

The secret of RSA is to work modulo pq, where p and q are (different) primes. We're going to need to do modular arithmetic mod pq, including exponentiation.

The details

So the only question is, how can we come up with such a system, where being able to encrypt things doesn't help you decrypt things very much?

The approach we'll describe was the first one to be thought of, in the 1970s. It is known as *RSA* after its American inventors Rivest, Shamir and Adleman. (A British mathematician, Cocks, invented it a few years earlier, but he was working in secret for the government, so this was not known for many years). RSA is still in very widespread use on the internet.

The secret of RSA is to work modulo pq, where p and q are (different) primes. We're going to need to do modular arithmetic mod pq, including exponentiation. So we'll need to see what Fermat-Euler says:

Fermat-Euler for pq

Fermat-Euler for pq

Proposition

Let p and q be different primes. Then the number $\varphi(pq)$, of integers between 1 and pq coprime to pq, is given by

$$\varphi(pq) = (p-1)(q-1).$$

Fermat-Euler for pq

Proposition

Let p and q be different primes. Then the number $\varphi(pq)$, of integers between 1 and pq coprime to pq, is given by

$$\varphi(pq) = (p-1)(q-1).$$

Proof.

?

□

Now we know $\phi(pq) = (p-1)(q-1)$

Now we know $\phi(pq) = (p-1)(q-1)$

Remark

As a result of that, we know (from the Fermat-Euler Theorem) that, for all a coprime to pq, we have

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

Now we know $\phi(pq) = (p-1)(q-1)$

Remark

As a result of that, we know (from the Fermat-Euler Theorem) that, for all a coprime to pq, we have

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq},$$

and indeed

$$a^{k(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

for all k.

Back to Alice and Bob

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve);

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d. He shreds any evidence of what p and q are.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.
He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.
His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d. He shreds any evidence of what p and q are.
Alice represents her message as a number m between 1 and pq.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d. He shreds any evidence of what p and q are.

Alice represents her message as a number m between 1 and pq. It is overwhelmingly likely that her choice will be coprime to pq.

Back to Alice and Bob

So, Bob chooses two fairly large primes p and q, and keeps them secret. He also chooses a number e which is coprime to $(p-1)(q-1)$.

He also calculates the inverse d to e, modulo $(p-1)(q-1)$, by using Euclid's algorithm.

His public key consists of pq and e, so he sends that to Alice (and Eve); his private key consists of pq and d. He shreds any evidence of what p and q are.

Alice represents her message as a number m between 1 and pq. It is overwhelmingly likely that her choice will be coprime to pq. She calculates

$$m^e \pmod{pq}$$

and sends it on to Bob.

Alice and Bob continued

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq.

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k.

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$(m^e)^d$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$(m^e)^d = m^{de}$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)}$$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)} = m(m^{\varphi(pq)})^k$$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)} = m(m^{\varphi(pq)})^k \equiv m1^k$$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)} = m(m^{\varphi(pq)})^k \equiv m1^k \equiv m \pmod{pq}.$$

Alice and Bob continued

Bob receives this number m^e from Alice, and raises it to the power d modulo pq. He thus obtains something congruent to

$$(m^e)^d = m^{de}.$$

Now, because $de \equiv 1 \pmod{\varphi(pq)}$, we have $de = 1 + k\varphi(pq)$ for some k. As a result,

$$(m^e)^d = m^{de} = m^{1+k\varphi(pq)} = m(m^{\varphi(pq)})^k \equiv m1^k \equiv m \pmod{pq}.$$

Hence, using his private key, Bob can recover what m was from being told m^e.

Security

Security

The idea is that it should be very hard for anyone else to work out d from pq and e;

Security

The idea is that it should be very hard for anyone else to work out d from pq and e; we did this using Euclid's algorithm, but we needed to know more than just pq: we needed to know $(p-1)(q-1)$.

Security

The idea is that it should be very hard for anyone else to work out d from pq and e; we did this using Euclid's algorithm, but we needed to know more than just pq: we needed to know $(p-1)(q-1)$.

So the security of this approach depends (among other things) on it being difficult to factorise the number pq:

Security

The idea is that it should be very hard for anyone else to work out d from pq and e; we did this using Euclid's algorithm, but we needed to know more than just pq: we needed to know $(p-1)(q-1)$.

So the security of this approach depends (among other things) on it being difficult to factorise the number pq: if factorising large numbers were easy, we could get p and q for ourselves from Bob's public key.

Security

The idea is that it should be very hard for anyone else to work out d from pq and e; we did this using Euclid's algorithm, but we needed to know more than just pq: we needed to know $(p-1)(q-1)$.

So the security of this approach depends (among other things) on it being difficult to factorise the number pq: if factorising large numbers were easy, we could get p and q for ourselves from Bob's public key. Currently, we know of no way to do this fast enough: we know how to generate primes that are hundreds of digits long, but not to factorise a product of two of them.

An example

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$.

An example

Let's see an example.

Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.

Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$.

An example

Let's see an example.

Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.

Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.
Suppose Alice decides she needs to send Bob message 1245,

An example

Let's see an example.
Suppose Bob has low opinions of Eve's calculational skills, and chooses to use the (unrealistically small) primes $p = 101$ and $q = 103$. Then $pq = 10403$. Suppose also that Bob chooses $e = 71$ for the exponent used for encryption.
Bob advertises that his public key is $pq = 10403$, $e = 71$. He must work out his private key, by inverting 71 modulo $(p-1)(q-1) = 10200$. A quick use of Euclid's algorithm will do this for him, and he gets that $71^{-1} \equiv 431$. Indeed,

$$71 \times 431 = 30601 = 3 \times 10200 + 1.$$

Thus his private key is $pq = 10403$, $d = 431$.
Suppose Alice decides she needs to send Bob message 1245, which they've agreed in advance should mean "please meet me after this lecture".

The calculations

The calculations

Then Alice has to calculate 1245^{71} modulo 10403.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$

$$\equiv 1245 \cdot 10381^{35}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35}$$
$$\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} &\equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ \equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}1245^{71} \equiv 1245 \cdot 1245^{70} &\equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} &\equiv 3819 \cdot (10381^2)^{17} \\ \equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} &\equiv 7065 \cdot (484^2)^8 \\ \equiv 7065 \cdot 5390^8 &\end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ \equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ \equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ &\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ &\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\ &\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4} \equiv 7065 \cdot 6924^{4} \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ \equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ \equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\ \equiv 7065 \cdot (6924^2)^2 \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4} \equiv 7065 \cdot 6924^{4} \\
\equiv 7065 \cdot (6924^2)^{2} \equiv 7065 \cdot 4752^{2}
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ &\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ &\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ &\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\ &\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\ &\equiv 7065 \cdot 6994 \end{aligned}$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4} \equiv 7065 \cdot 6924^{4} \\
\equiv 7065 \cdot (6924^2)^{2} \equiv 7065 \cdot 4752^{2} \\
\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}
$$

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$
\begin{aligned}
1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\
&\equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\
&\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^{8} \\
&\equiv 7065 \cdot 5390^{8} \equiv 7065 \cdot (5390^2)^{4} \equiv 7065 \cdot 6924^{4} \\
&\equiv 7065 \cdot (6924^2)^{2} \equiv 7065 \cdot 4752^{2} \\
&\equiv 7065 \cdot 6994 \equiv 8763.
\end{aligned}
$$

So she sends Bob 8763.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned} 1245^{71} \equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} \equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ \equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ \equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\ \equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\ \equiv 7065 \cdot 6994 \equiv 8763. \end{aligned}$$

So she sends Bob 8763.
Bob receives this, and his task then is to calculate 8763^{431} modulo 10403.

The calculations

Then Alice has to calculate 1245^{71} modulo 10403. This sounds scary, but she can do it fairly quickly if she's careful:

$$\begin{aligned}1245^{71} &\equiv 1245 \cdot 1245^{70} \equiv 1245 \cdot (1245^2)^{35} \\ \equiv 1245 \cdot 10381^{35} &\equiv 1245 \cdot 10381 \cdot 10381^{34} \equiv 3819 \cdot (10381^2)^{17} \\ &\equiv 3819 \cdot 484^{17} \equiv 3819 \cdot 484 \cdot 484^{16} \equiv 7065 \cdot (484^2)^8 \\ &\equiv 7065 \cdot 5390^8 \equiv 7065 \cdot (5390^2)^4 \equiv 7065 \cdot 6924^4 \\ &\equiv 7065 \cdot (6924^2)^2 \equiv 7065 \cdot 4752^2 \\ &\equiv 7065 \cdot 6994 \equiv 8763.\end{aligned}$$

So she sends Bob 8763.
Bob receives this, and his task then is to calculate 8763^{431} modulo 10403. A similar strategy makes this possible, too, and he finds that

$$8763^{431} \equiv 1245 \pmod{10403},$$

so he has reconstructed Alice's message.

Square roots of 2

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it?

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it? Why should we feel that $\mathbb{Q}$ is not enough?

Square roots of 2

We've spent nine lectures now talking about $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$, laying the foundations of number theory. The rest of this course will be about $\mathbb{R}$. Perhaps sensibly enough, the study of $\mathbb{R}$ is called *real analysis*.

Let's set ourselves back to a time before $\mathbb{R}$ was invented, and ask: why was it necessary to invent it? Why should we feel that $\mathbb{Q}$ is not enough?

The result that set the ancient Greeks thinking was this:

Theorem

There is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof.

?

□