The Magic Keys of Esprenevestos

An Analogy of Public Key Encryption for Kids

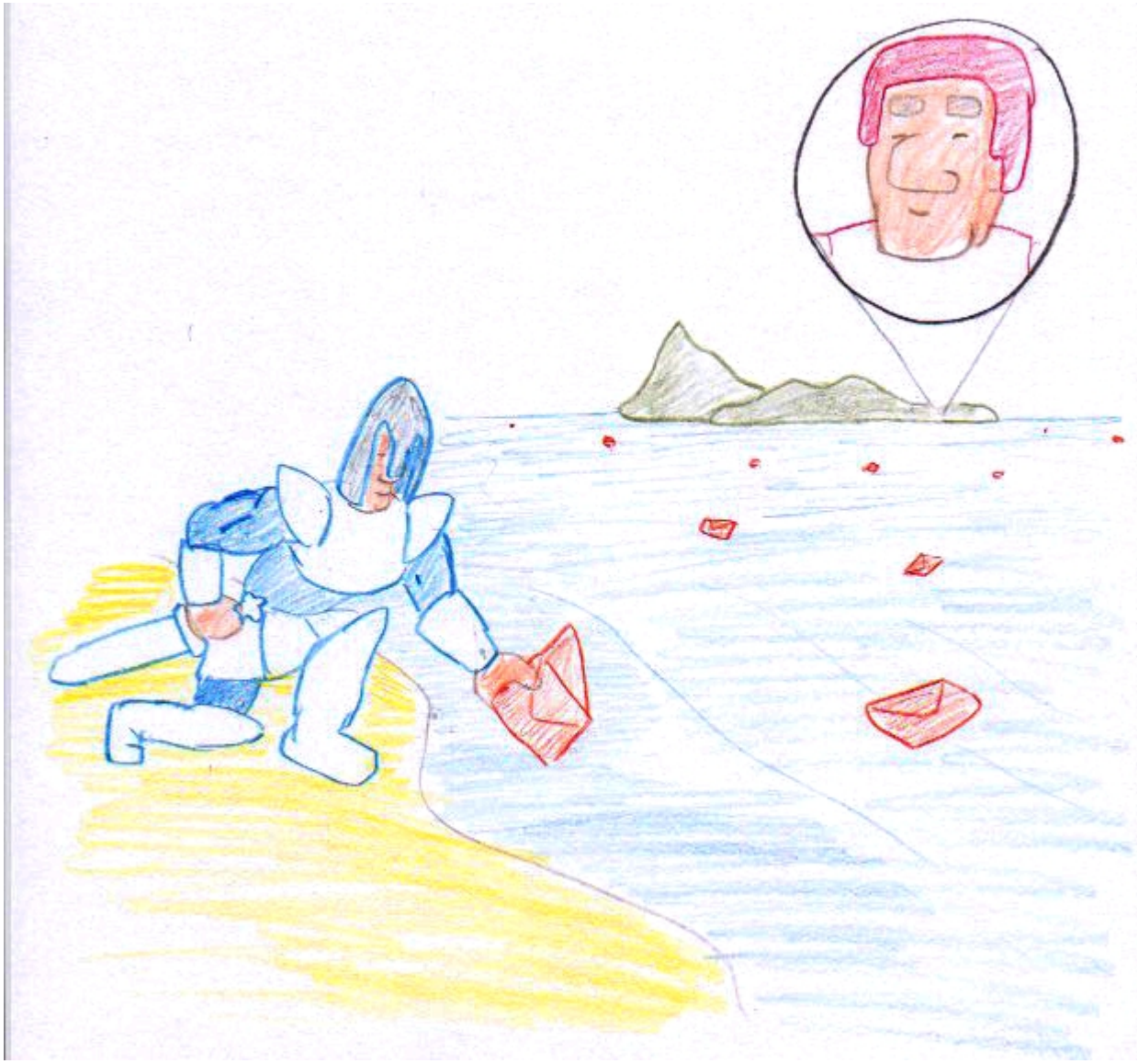
This story introduces some key concepts of how data is sent securely over the Internet, including: public and private keys, digital signatures, and certificate authorities... Although it mostly replaces the word “digital” with “magical”.

Read the explanation after the story if you're interested in the science; otherwise just enjoy the story.

Version 0.2.1

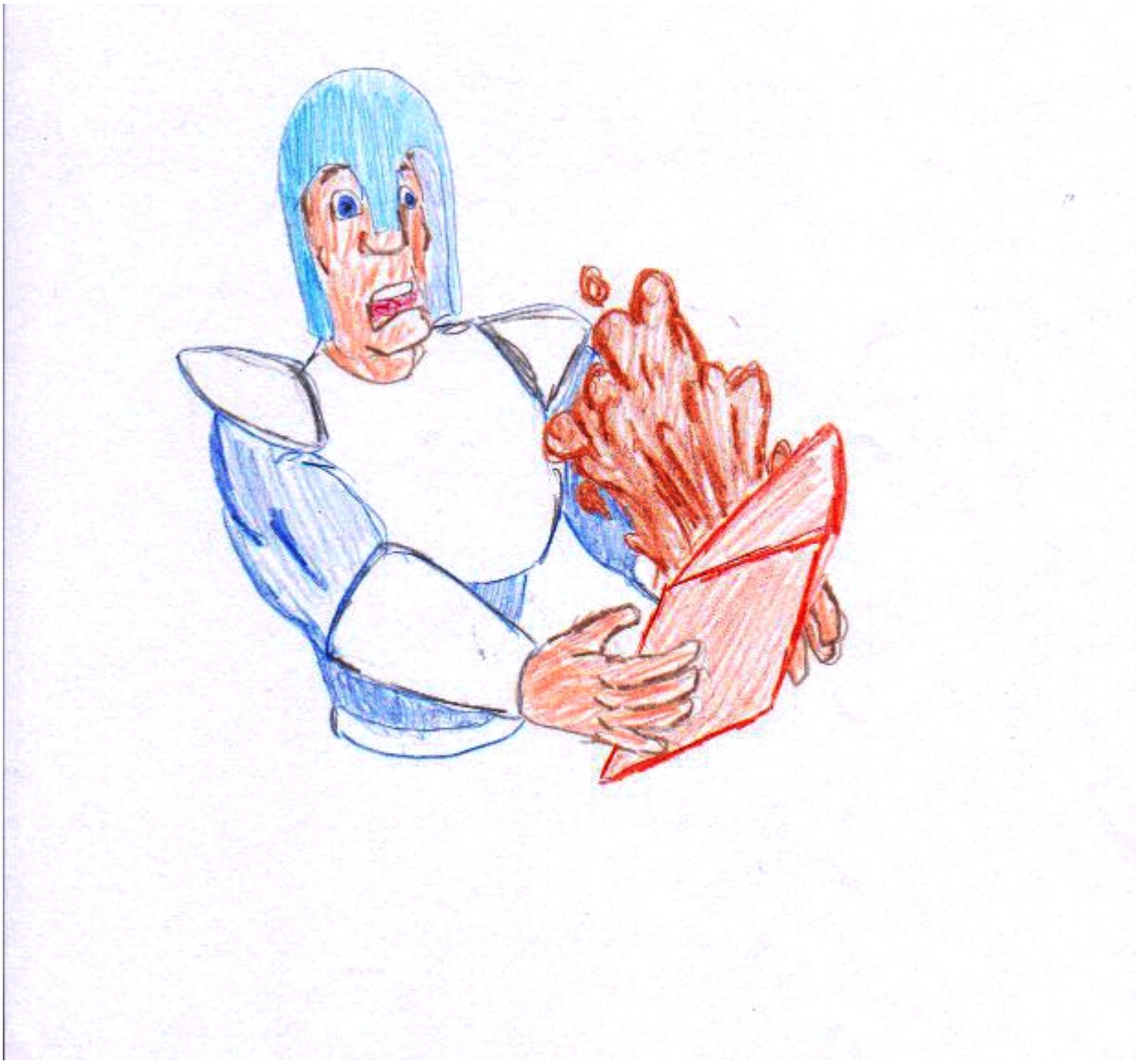
By Michael Nelson

In the Kingdom of Esprenevestos there lived two knights, Sir Comilujo and Sir Jon, who were separated by a large sea. In this sea, there were mysterious floating packets which were carried with the tide from one side to the other. Some people said they were placed there by mermaids, but no one was certain.



One day, Comilujo put a letter for Jon inside a packet and set it adrift in the sea. A few days later, Jon found it, read it, and sent a reply in another packet back to Comilujo.

Sending packets like this worked really well. Pretty soon, everyone was using these packets to send all sorts of things: letters, paintings, and even gold coins.



One day, Comilujo found a packet from Jon, but when he opened it brown sludge jumped out.“Yuck! What is this and why did Jon send it to me?”

Comilujo went to the magician Algamel for answers.

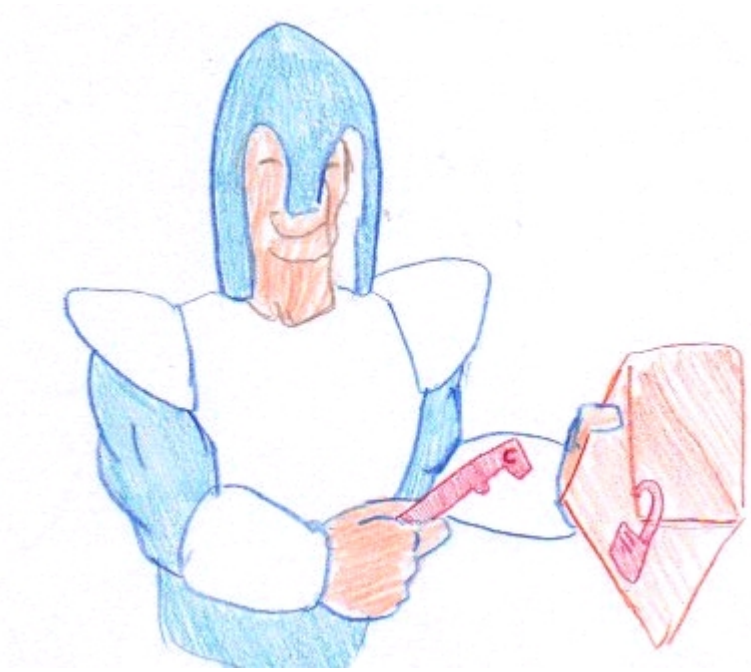
Algamel told him the sludge was a virus, but, with an expensive antidote, he could be cured. Also, the message wasn't actually from Jon.
“This is the doing of Hackbeard the Pirate! He must have found Jon's packet and put the virus in it.”

Now everyone was scared to open packets.
But, Algamel had a plan: he cast a spell that created 2 pairs of magic keys: a Red key and Green key for Comilujo, and a Red key and Green key for Jon. Their Green key could close any lock, and then the lock could only be opened by their Red key.

So a lock closed by Comilujo's Green key could only be opened by his Red key; and a lock closed by Jon's Green key could only be opened by Jon's Red key.

Comilujo and Jon couldn't wait to use their new keys! They created many copies of their Green key, and sent them in packets to all their friends, including each other.

Next time Jon sent a packet to Comilujo, he put a lock on it, and closed it with the Green key he got from Comilujo.



When Comilujo got the packet, he opened it with his own Red key.

It didn't matter if pirates found the packet before Comilujo because they couldn't open it, they didn't have the right Red key.

Comilujo sent packets safely to Jon the same way.

A few days later, Comilujo opened a packet using his Red key, and out jumped the brown sludge again!

He went to see Algamel again. “Your magic keys don't work. Hackbeard still put a virus in a packet from Jon!”
“I see... but how do you know the packet was from Jon? You sent copies of your Green key to everyone. Hackbeard must have got a copy of your Green key, too, and used it to lock the packet, and then pretended it was sent by Jon.”

“I didn't get a chance to tell you”, Algamel continued, “each of your Red keys can do other magic. It can write a magic signature on the packet, and when you wave its Green key over the signature, the key will speak the word 'Verified!'. A Green key will only do this for a message signed by its Red key.”

So, next time Jon sent a packet to Comilujo, he gave it a magic signature with his Red key, then locked the packet with the Comilujo's Green key.

When Comilujo found the packet, he waved Jon's Green key over it, heard it say “Verified!”, and then opened it with his Red key.

Now they could send packets safely!

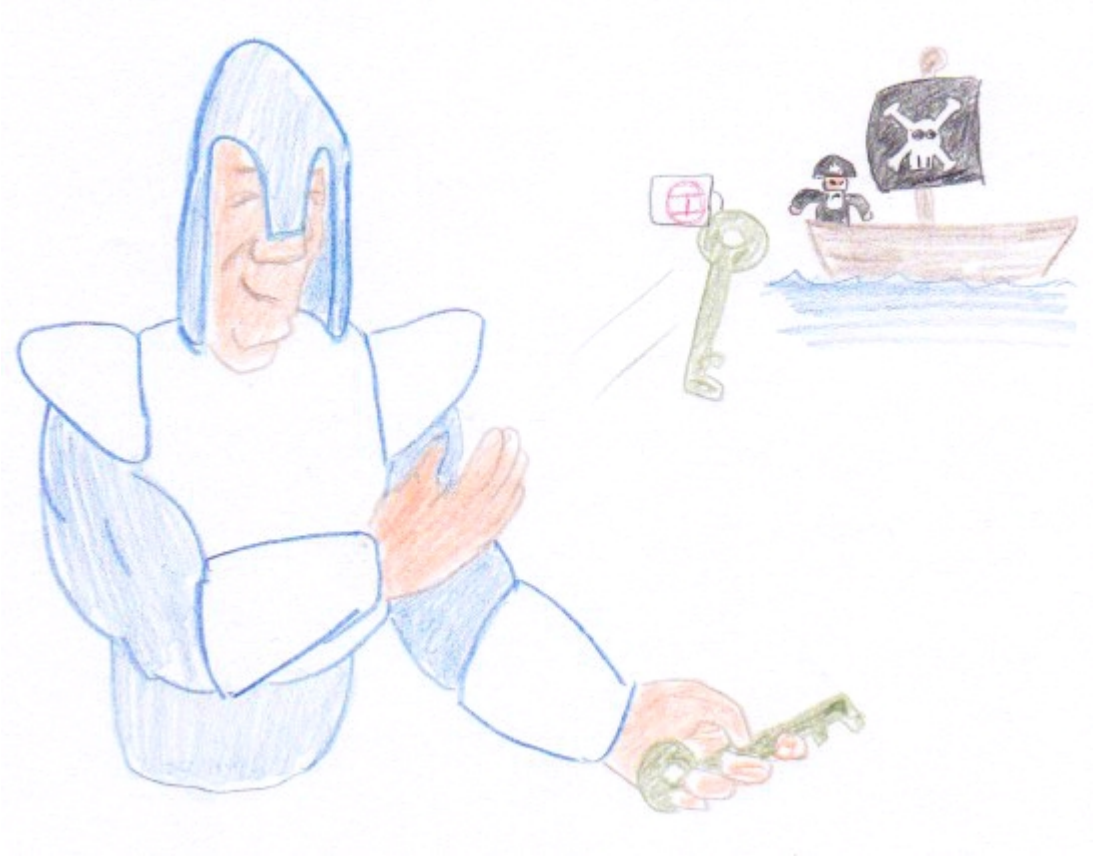
One day Comilujo was opening another packet from Jon when brown sludge jumped out and covered him! Then it continued to spread throughout the city. Then he heard the sound pirates attacking!

Just when it appeared the pirates would overrun the land, the magician Algamel came and cast a spell that stopped the spread of the brown sludge, and Comilujo and the other knights were able to fight the pirates out of their land.
The pirates retreated, but vowed to return again in even greater numbers.

When the fighting was over, Comilujo asked Algamel:
“I did exactly as you said- but the pirates still managed to fool Jon's Green key into thinking the packet was from him!”
“I see... but how do you know the Green key you were using was actually from Jon?”
“Well, I got it in a packet that said it was from him...”
“I'm afraid the key you thought was from Jon was actually from Hackbeard the Pirate. He must have learned how to create the magic keys, too.”
“So every time that key said a message was from Jon, it was actually from Hackbeard! So how can we trust someone's Green key, if we can't be sure they actually sent it? Any Green key ever sent could be from a pirate!”

Algamel had a final plan. He travelled throughout the land, attaching magical certificates on everyone's real Green keys. The certificate had Algamel's signature on it, written by his own Red key. He then gave them a copy of his Green key. When they waved his Green key over the certificate, it would verify the signature was his and say the key owner's name.
This way they could know who really owned the Green key.

Later, Comilujo received a packet with another Green key in it that said it was from Jon. But when he waved Algamel's Green key over its certificate, it didn't say anything. “Hmmm, this key must not be from Jon, otherwise Algamel's key would have said so... I think this is from Hackbeard, again.” So he threw the key in the garbage.
Off in the distance, he could see Hackbeard's ship. “Nice try!” he called to them.



So Hackbeard couldn't trick people into using his Green key. He didn't have others' Red keys either, so he couldn't open their packets or write their magic signatures to pretend packets were from them. He couldn't do anything!
He eventually took a job as Algamel's helper.

A few days later Comilujo received another packet with a key saying it was from Jon. This time, as he waved Algamel's key over the certificate, it said “Verified! Sir Jon”. So he knew this Green key was actually from Jon!
Now that Comilujo had Jon's real Green key, he could use it to lock packets and send them to Jon, and it told him when packets were actually from him too.
Jon got Comilujos' Green key too, so he could do the same.
With each others' Green keys, they never had problems sending packets again.

The End

Real Public Key Cryptography

In real public key cryptography, there are two users who want to send messages safely over the internet (just like how Comilujo and Jon wanted to send packets over the sea).
Unfortunately, these messages can be read by others, and the contents can be changed by them too (just like how Jon's message could be read by pirates, and its contents were replaced with a virus).
In order to prevent this, each user can create cryptographic public and private keys using their computers (the math is pretty complex but you can learn it if you want). These keys are actually special numbers that are extremely hard to guess. The public key can be used to encrypt a message so that the only way it can be read is by using its corresponding private key (just like Comilujo's Green key could lock a packet so that only his Red key could unlock it).
So if you give someone your public key, they can send messages to you, knowing that no one else in the world can read them because it can only be decrypted using your private key, which key you never share (hence why it's called “private”). This way you can distribute your public key with everyone, so anyone in the world can send you an encrypted message and know only you will be able to read it. The only trouble is you have no way of knowing for sure who sent the message.
This is where signatures come into play. Private keys can also be used to create a digital signature which gets sent along with messages (just like Jon created a magic signature on the packet using his Red key). Digital signatures are essentially another number that gets encoded with a private key. This digital signature can only be decoded by the corresponding public key (just like Comilujo used Jon's Green key verified the packet was from him) . If a digital signature is decoded by a public key, you can know for certainty it was signed by the corresponding private key. This is how digital signatures are verified.
So when sending a message, the sender adds a digital signature using their private key, and they encode the entire message using the recipient's public key. Then the recipient decodes the message using their private key (no one can do this because no one else has their private key) and they verify the sender's signature using the sender's public key (anyone can do this because the sender's public key is freely available, but only the sender could have created the signature).
The last remaining problem is: how do the sender and receiver initially exchange their public keys? They could send each other an email with their public key in it, but normal email has the same problem: others can read it and even change it.
This is where certificate authorities come into play. Although anyone with a computer can create the public/private keys (just like, in the story, the pirates learned how to make the keys), someone needs to confirm a public key actually belongs to someone, otherwise it can't be trusted.
So instead, certificate authorities create the public/private keys, do a lot of work to keep them safe, and people get these keys from them (just like, in the story, everyone got their keys from Algamel). With any pairs of public keys they hand out, they will give an accompanying certificate, which contains information about the new key's owner, and is signed by the Certificate Authority's private key.
So in order to verify a public key's owner, someone just uses the Certificate Authority's public key to read the certificate.
So then how do we get the Certificate Authorities' public keys? We can't request them insecurely over the internet. Those have to come pre-installed in the computer or software. (Just like Algamel handed out copies of his Green key personally to everyone at the end.)
So the complete process for using public key cryptography to send packets safely is this:

1. Your computer and the recipient's computer come pre-installed with the certificate authority's public key
2. You both get a public and private key from a certificate authority
3. Your computer sends a message to the computer you want to communicate with, which includes

your public key and its certificate, and asking for their public key
4. The recipient's computer verifies your public key using the certificate authority's public key
5. The recipient's computer sends you their public key with its certificate
6. Your computer verifies their public key's certificate using the certificate authority's public key
7. Your computer uses their public key to encrypt your message
8. Your computer signs the message with your private key
9. The message is sent to the recipient
10. The recipient's computer verifies the signature using your public key
11. The recipient's computer decrypts the message using their private key
12. The recipient's computer reads the message
13. For subsequent messages, repeat steps 7-12

If you have feedback or suggestions, please let me know on cmljnelson.wordpress.com