Cryptography - 2

Sensei Glen | Code Ninjas

So Far..

We've learnt about:

- Private Keys
- Public Keys
- How encrypting and decrypting works
- How to GENERATE our own Keys!
- Decrypting each others' names

01

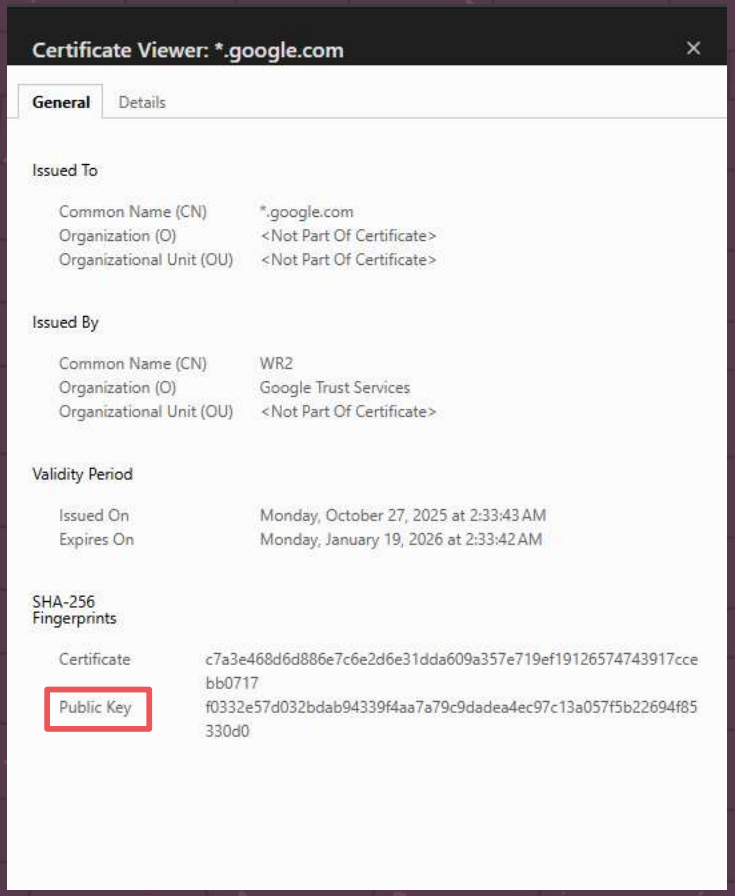
What About Some Real Life Examples?

Checking Our Browser's Cryptography in Action

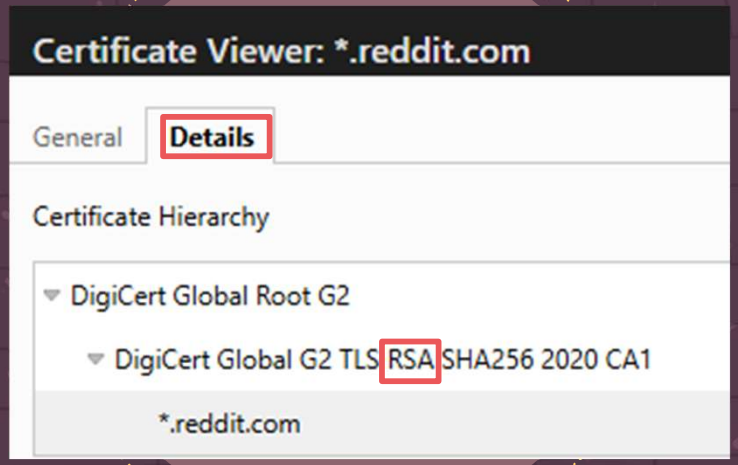
Everyday websites use cryptography to ensure hackers don't get your information easily, and to help internet users surf websites without worrying about data leakages.

One such example is **Google** (but you can go to any website, really) which shows you your encryption key, but smartly keeps the private key hidden!

Google uses an SHA-256 encryption which works with a hash function.



A Few More Examples



Even though Google uses SHA-256, a lot of websites use different methods of encryption, depending on user needs.

One such example is **Reddit,** which uses a combination of **RSA**, **TLS** (Transport Layer Security) and **SHA-256** (Secure Hash Algorithm) to ensure extra safe browsing on the platform!

Activity!

I want all of you to:

- Go to your favourite website
- Try and spot the Encryption (Public) key, and what kind of cryptosystem is in use for the same.
- After this, find **at least 2** websites using either **RSA**, **TLC**, or **SHA-256.**
- Let a Sensei know once you're done!

Awesome Work!

We see that Cryptography has large scale applications in the real world, especially to keep our information safe.

02

SIGNATURES!

How Do We Know who the Sender Is?

So we've figured out how to encrypt messages. However, how do we **Verify** if it is actually sent by the right person?

- This is where RSA Signatures come in.
- Encryption keeps messages secret, but Signatures prove **people** are **real**.

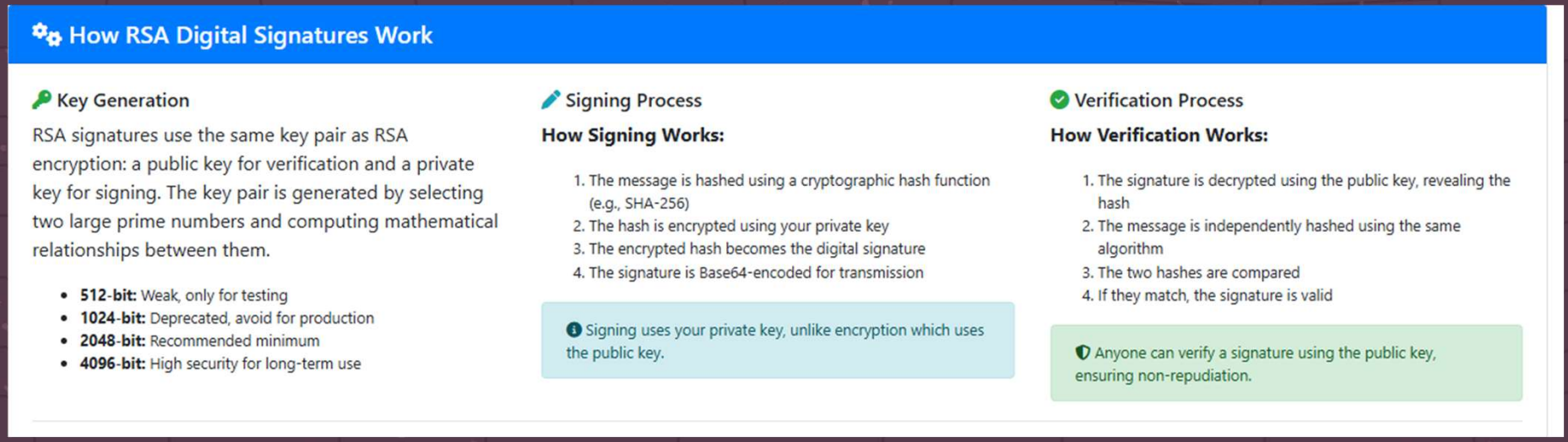
If I sign something with my private key,

- Anyone can check the signature with my public key
- But only ***I*** could've created it..
- It proves that the message is authentic and is actually sent by me.

Let's Learn with an Activity

Look to your Python Notebook, there are a few links for activities!

The first one leads you to the Signature Verifying website, where all of us can play around with exchanging messages.



Signatures Protect you From:

- Fake Websites
- Malware Pretending to be apps
- Tampered Files
- Impersonation
- Inaccurate Information

03

Steganography

Steganography – What is it?

Steganography is the practice of *hiding* a message inside of something that looks normal.
We're not **scrambling** the message, that would be encryption.
We're simply hiding it into, say for example, an image!

Steganography – What is it?

You could hide text inside of:

- images
- audios
- a PDF

and the file would look the **exact same** to the human eye.

But.....

If you knew how to extract the data somehow...

The secret message appears!

SteganoGraphy Activity

Let's now look to our Python Notebook and follow the Sensei's instructions on what to do with this peculiar image…….

04

Conclusion

So, What did we Learn Today..

- Did a recap from last week on the RSA Cryptosystem from last week on Python.
- Explored a bunch of websites using different Encryptions.
- Discovered the idea of Verification and Signatures!
- Exchanged messages with Signing them!
- Uncovering hidden messages in images through Steganography!

THANK YOU

It has been an absolute pleasure teaching all of you!!

glenissac392@gmail.com
+1 (639) 554-5833
github.com/gelnerr

RESOURCES

1. Rivest-Shamir-Adleman Photo
2. Lebron James you are my Sunshine
3. Monkey looking away template