

Hybrid crypto interactive Lecture 12b: 2022-04-06

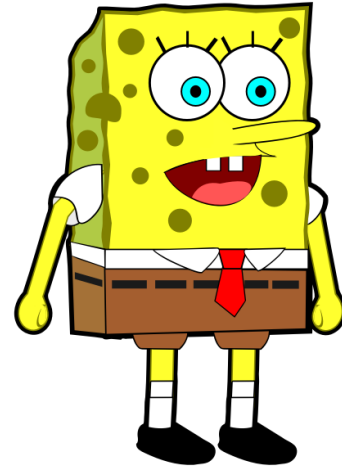
MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

A Communications Story



(A)lice from Alice's Adventures in Wonderland
Illustration by Arthur Rackham, 1907



Sponge(B)ob Squarepants
<https://freesvg.org/sponge-bob-squarepant>



(E)ve by Lucas Cranach the Elder (1528)

Symmetric vs asymmetric crypto

Symmetric encryption



- Uses same key for encryption and decryption.
- Fast, but doesn't work if Eve is able to intercept the key.
- Examples: Caesar cipher, Vigenère cipher, AES/Rijndael (2001)

Asymmetric encryption



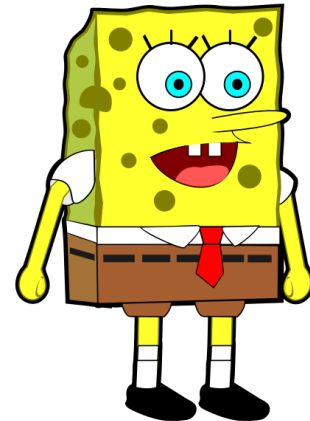
- A.k.a. public-key crypto
- Knowing how to encrypt doesn't tell you how to decrypt.
- Slow, because lots of math, but able to secure communications even if Eve hears everything.
- Examples: RSA, ElGamal

Hybrid cryptosystems

- We can get the best of both worlds by combining the two.
- Use the slow public-key cryptography (e.g. RSA) to exchange a small message containing a key for the symmetric method.
- Then use the fast symmetric encryption method (e.g. AES) for everything else.



Old El Paso advertisement; Mia Agraviador pictured



Real-life example

The image shows a web browser window displaying the University of Toronto website. A security warning is visible in the address bar, indicating a secure connection. A 'Page Info' window is open, showing details about the website's identity, privacy, and technical details.

Browser Address Bar: University of Toronto | <https://www.utoronto.ca>

Security Warning: Connection security for www.utoronto.ca
You are securely connected to this site.
Verified by: Sectigo Limited
More information

Page Info — <https://www.utoronto.ca/>

Website Identity

- Website: www.utoronto.ca
- Owner: This website does not supply ownership information.
- Verified by: Sectigo Limited [View Certificate](#)
- Expires on: Friday, March 17, 2023

Privacy & History

- Have I visited this website prior to today? Yes, 3 times
- Is this website storing information on my computer? Yes, cookies and 746 bytes of site data [Clear Cookies and Site Data](#)
- Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

- Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
- The page you are viewing was encrypted before being transmitted over the Internet.
- Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

Real-life example

The screenshot shows a Firefox browser window with the address bar displaying the URL: `about:certificate?cert=MIIHCTCCBfGgAwIBAgIRAPUXn4hnOiz8Qf3%2BCkhWJIQwDQYJKoZIhvcNAQELBQ`. The browser tabs include "University of Toronto" and "Certificate for www.utoronto.ca". The main content area displays the following certificate information:

Validity	
Not Before	Thu, 17 Mar 2022 00:00:00 GMT
Not After	Fri, 17 Mar 2023 23:59:59 GMT
Subject Alt Names	
DNS Name	www.utoronto.ca
DNS Name	utoronto.ca
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	A2:2B:BA:27:C0:90:BC:AC:12:18:35:31:9D:08:0A:27:83:06:3E:4B:FF:1A:0E:87:83:7...
Miscellaneous	
Serial Number	00:F5:17:9F:88:67:3A:2C:FC:41:FD:FE:0A:48:56:24:84
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	E7:71:DA:7F:6D:53:78:2A:4D:1C:CD:9A:22:2E:40:C2:EC:B3:50:5B:D3:E7:0B:B5:65:...

Toy example

- Alice: Hello there!
- Bob: generate RSA modulus/exponent
- Bob: sends public key
- Alice: choose symmetric key
- Alice: send RSA-encrypted symmetric key to Bob
- Bob: decrypts to get symmetric key
- Both: communicate using symmetric key and cipher.

Interactive exercise (groups of 3-5)

Part 1:

- Generate an RSA modulus n using 2-digit primes.
- Choose an exponent k such that $\gcd(k, \phi(n)) = 1$
- Choose a Caesar cipher key $a > 1$ with $\gcd(a, n) = 1$
- Encrypt the Caesar cipher key by $b \equiv a^k \pmod{n}$
- Write a short message of 15-30 characters.
- Encrypt the message using the Caesar cipher key a .
- Publish the message (n, k, b) and encrypted msg!

Part 2:

- Decrypt other groups messages.
- First compute $a \equiv \sqrt[k]{b} \pmod{n}$
- Then use Caesar cipher key to decrypt the message.

Conclusion to Magic of Numbers

- What really are numbers?
- Where did math come from?
- Why did we invent so many numbers and operations?



- How do you think like a mathematician?
- What are some other types of number systems?
- How does the magic of numbers affect our lives?