Public-Key Cryptography Lecture 12a: 2022-04-04

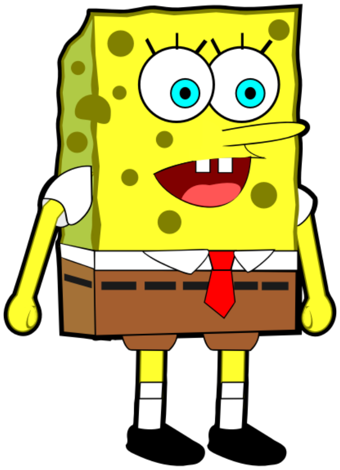
MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

A Communications Story

A

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



B

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

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

Eavesdropper

Symmetric ciphers

- Caesar shift: add a number to every letter mod 26.
  - The number you add is the "key".
  - If you know the key, you can both encrypt and decrypt.

Ex. YES , key = 2 (B)

Encrypt 25, 05, 19 $\xrightarrow[+2]{}$ ~~27~~ 01, 07, 21 AGU

Decrypt 01, 07, 21 $\xrightarrow[-2]{}$ 25, 05, 19 YES

- Vigenère cipher: add a cyclically repeating word to the message mod 26.
  - The word you add is the "key".
  - If you know the key, you can both encrypt and decrypt.

Ex. TORONTO , key = CN

Encrypt:

TORONTO
+ CNCNCNC
WCUCQHR

Decrypt

WCUCQHR
− CNCNCNC
TORONTO

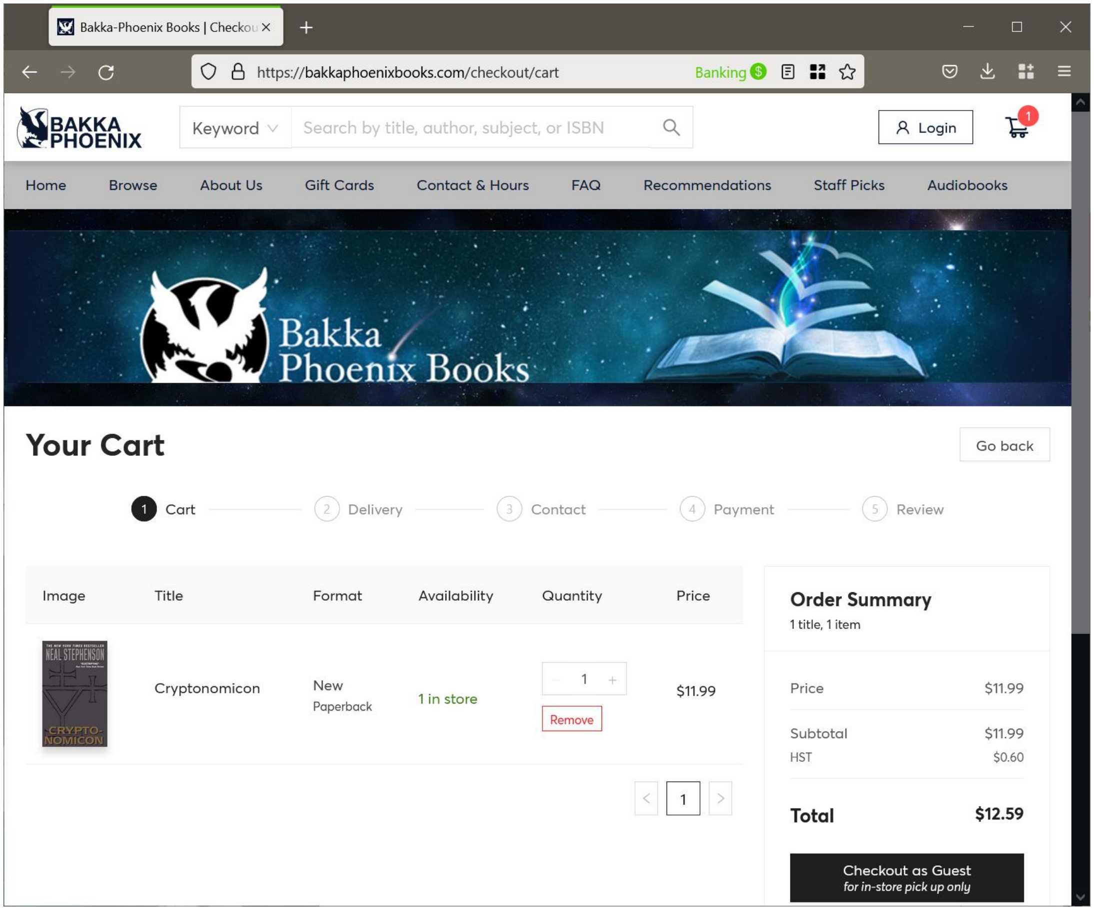
Symmetric ciphers and eavesdropping

- Symmetric ciphers use the same key for encryption and decryption.
- They only work when Eve only hears part of the conversation.
- If Eve ever hears the key, then she can decrypt the entire conversation, both past and present.

Johann Georg Meyer von Bremen
(Germany, 1813 - 1886)

Beating a perfect eavesdropper

- What if Eve knows everything Alice and Bob have ever said to each other, so there’s no way for them to share a secret key without Eve knowing?
- In fact, let’s say that Alice and Bob have never even met, but are just communicating on the Internet.



Asymmetric encryption

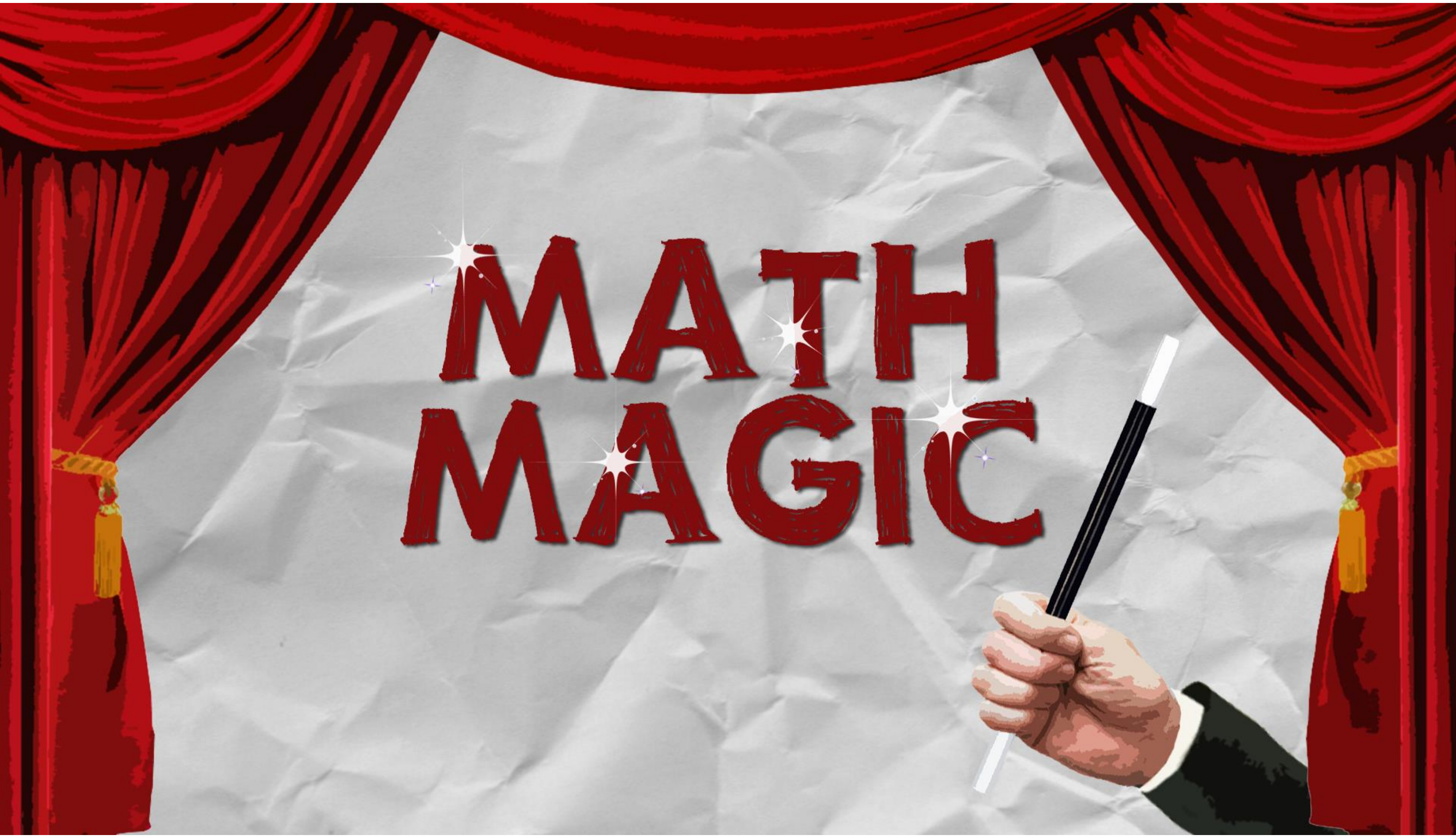
- What if encryption and decryption use different keys? Or if encryption doesn't need a secret at all?

Symmetric encryption

Asymmetric encryption

public key

- Then, Bob could give everyone the encryption key, but not tell anyone the decryption key. private key



https://www.pbslearningmedia.org/resource/42439c47-de30-487c-9c10-563367a2c843/math-magic/

Reversing is hard: factoring

- We define addition, multiplication, exponentiation, etc, and those are easy.

$4931 \cdot 7919$

$= 9048589$

- Subtraction, division, and roots, are reversing those operations and sometimes much harder.

Factoring is hard

(even testing if prime accurately is hard)

https://www.flickr.com/photos/nenadstojkovic/50446472706/in/photostream/

Floris de Wit; https://dribbble.com/shots/5039546-Moonwalk

Factoring large numbers

- Figuring out if a number is prime is "easy" using probabilistic primality testing (e.g. Fermat)
  - We want to know if n is prime.
  1. Pick a random number a between 1 and $n-1$
  2. Compute $a^{n-1} \pmod{n}$
  3. If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime and a is a witness to this fact. Otherwise, n passes the test, and you don't know for certain, but you can repeat.

$2^{142} \bmod 143 \equiv 114 \bmod 143$, so 143 is not prime

- Factoring a composite number is "hard" for large numbers if you don't know any divisors.

143

11 13

might need to test all prime up to $\sqrt{143}$

Finding roots with Euler's Theorem

- Algorithm for $\sqrt[k]{a} \pmod{n}$ using Euler's Theorem
  - Conditions: $\gcd(a, n) = 1$ and $\gcd(k, \phi(n)) = 1$.

Ex. $\sqrt[3]{7} \bmod 15$ $15 = 3 \cdot 5$ $\gcd(7, 15) = 1$ $\phi(15) = 8$ $\gcd(3, 8) = 1$

  - Find 1 as a combination of k and $\phi(n)$

$$1 = km - l\phi(n)$$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2$

$1 = 3 - (8 - 3 \cdot 2)$

$1 = 3 \cdot 3 - 8$

$1 + 8 = 3 \cdot \underset{m}{\underset{\uparrow}{3}}$

  - Then $a^1 \equiv a^{1 + l\phi(n)} \equiv a^{km}$.

$7^1 \equiv 7^9$ because $7^8 \equiv 1$ by Euler's Thm. mod 15

  - So $\sqrt[k]{a} \equiv \sqrt[k]{a^{km}} \equiv a^m \pmod{n}$

$\sqrt[3]{7} \equiv \sqrt[3]{7^9} \equiv 7^{9 \cdot \frac{1}{3}} \equiv 7^3 \equiv 49 \cdot 7 \equiv 4 \cdot 7 \equiv 28$

$\equiv 13 \mod 15$

Reversing is hard: roots

- Computing $a^k \pmod{n}$ ~~is~~ needs a, k, n.

Ex. $13^3 \bmod 15 \equiv (-2)^3 \equiv -8 \equiv 7 \bmod 15$

- Computing $\sqrt[k]{a} \pmod{n}$ is needs $a, k, n, \underbrace{\phi(n)}_{\text{hard because factoring is hard}}$.

$\sqrt[3]{7} \bmod 15$

$\equiv 13 \bmod 15$

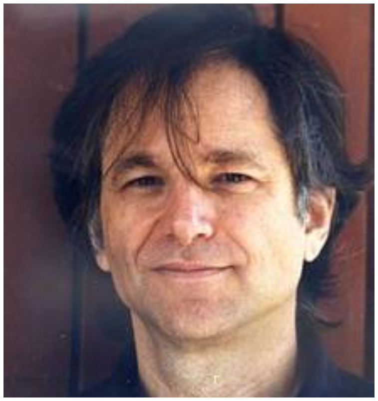
(see prev. slide)

RSA (Rivest-Shamir-Adleman, 1977)

- First public-key cryptosystem, which allows two parties who have never communicated before to send messages securely to each other.
- Made internet shopping and banking possible, because you can communicate securely with other computers without worrying about eavesdroppers.

Ron Rivest

Adi Shamir



Leonard Adleman

RSA algorithm

1. Alice introduces herself to Bob.
2. Bob generates a two large random primes, $\boxed{p, q}$ and computes the product $n = pq$ secret
3. Bob chooses an exponent k with $\gcd\big(k, \phi(n)\big) = 1$.
4. Bob sends (n, k) to Alice as a public key. Anyone who knows the public key can send messages to Bob that only he can decrypt.
5. Alice has a message a, with $\gcd(a, n) = 1$, so she sends $b \equiv a^k \pmod{n}$ to Bob
6. Bob can decrypt $a \equiv \sqrt[k]{b} \pmod{n}$

Example

Alice message: $a = 42$

1. Alice introduces herself to Bob.
2. Bob generates a two large random primes, p, q and computes the product $n = pq$
3. Bob chooses an exponent k with $\gcd(k, \phi(n)) = 1$.
4. Bob sends (n, k) to Alice as a public key. Anyone who knows the public key can send messages to Bob that only he can decrypt.
5. Alice has a message a, with $\gcd(a, n) = 1$, so she sends $b \equiv a^k \pmod{n}$ to Bob
6. Bob can decrypt $a \equiv \sqrt[k]{b} \pmod{n}$

$\left.\begin{array}{l} p = 4931 \\ q = 7919 \end{array}\right\}$ Find using Fermat primality test

$n = 9048589$

$\phi(n) = n \cdot \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)$

$= (p-1)(q-1)$

$k = 23$

public key: $(9048589, 23)$

$b \equiv 42^{23} \mod n$

$a = \sqrt[23]{b}$ (because Bob knows $\phi(n)$)

Example

- Alice wants to send the message “196” to Bob, but don’t want eavesdroppers knowing.
- Bob generates two prime numbers, 19 and 23, which he keeps as his secret key. $19 \cdot 23 = 437$
- He also chooses 61 as his exponent. Then he publishes (437, 61) as his public key.
- Alice sends $196^{61} \pmod{437} \equiv \boxed{9}$ to Bob.
- Bob can then decrypt the message because he knows the factorization of $437 = 19 \cdot 23$, so he can compute $\phi(437) = 19 \cdot 23 \cdot \frac{18}{19} \cdot \frac{22}{23} = 18 \cdot 22 = 396$
- Eve cannot decrypt the message unless she is able to factor 437.

Decryption in detail

- Eve intercepts an encrypted message "9" sent to a public key (437, 61).
- Being really clever, Eve breaks the private key and figure out that $437 = 19 \times 23$.
- What was the original unencrypted message?

Need to compute $\sqrt[61]{9} \mod 437$

$\phi(437) = 18 \cdot 22 = 396$

$396 = 61 \cdot 6 + 30$

$61 = 30 \cdot 2 + 1$

$30 = 30 \cdot 1$

$1 = 61 - 30 \cdot 2$

$1 = 61 - (396 - 61 \cdot 6) \cdot 2$

$1 = 61 \cdot 13 - 396 \cdot 2$

$t \quad m$

$\sqrt[61]{9} \equiv 9^{13} \mod 437$

$\equiv 9^8 \cdot 9^4 \cdot 9^1$

$9^1 \equiv 9$

$9^2 \equiv 81$

$9^4 \equiv 6$

$9^8 \equiv 36$

$\equiv 36 \cdot 6 \cdot 9$

$\equiv \boxed{196}$

Try it out: encryption

- Encrypt the message 9 using the RSA public key $(n, k) = (77, 13)$, without factoring 77.

$\gcd(9, 77) = 1$

$\gcd(13, 60) = 1$

$$9^{13} \bmod 77 \equiv 9^8 \cdot 9^4 \cdot 9$$
$$\equiv 25 \cdot 16 \cdot 9$$
$$\equiv 400 \cdot 9$$
$$\equiv 15 \cdot 9$$
$$\equiv 135$$
$$\equiv 58 \bmod 77$$

$9^1 \equiv 9$

$9^2 \equiv 81 \equiv 4$

$9^4 \equiv 16$

$9^8 \equiv 256 \equiv 25$

$$\begin{array}{r} 77 \\ \times 3 \\ \hline 21 \\ 21 \\ \hline 231 \end{array} \qquad \begin{array}{r} 77 \\ \times 5 \\ \hline 35 \\ 35 \\ \hline 385 \end{array} \qquad \begin{array}{r} 135 \\ -77 \\ \hline 58 \end{array}$$

A: 12
B: 23
C: 58
D: 70
E: None of the above

Try it out: decryption

- Decrypt a message encrypted using the RSA public key $(n, k) = (77, 13)$, with secret key $77 = 7 \cdot 11$.
- The encrypted message is 26.
- Helpful hint: $1 = 60 \cdot 5 - 23 \cdot 13$

$a^{13} \equiv 26 \mod 77$

$a \equiv \sqrt[13]{26} \mod 77$

$\phi(77) = 6 \cdot 10 = 60$

$\gcd(26, 77) = 1$

$\gcd(13, 60) = 1$

$\sqrt[13]{26} \equiv \sqrt[13]{26^{-23 \cdot 13}}$

$\equiv 26^{-23} \equiv 26^{37}$

$26^1 \equiv 26$

$26^2 \equiv 676 \equiv 676 - 616 \equiv 60 \equiv -17$

$\vdots$

$26^{37} \equiv 5$

A: 5
B: 12
C: 34
D: 67
E: None of the above

Hybrid cryptosystems

- Public-private key encryption is often a lot harder than symmetric key encryption.
- This is true even for computers, which can do both, but are much slower at public-key encryption.
- Thus, in practice, Alice and Bob only use RSA to send a very short message containing a key for symmetric encryption.