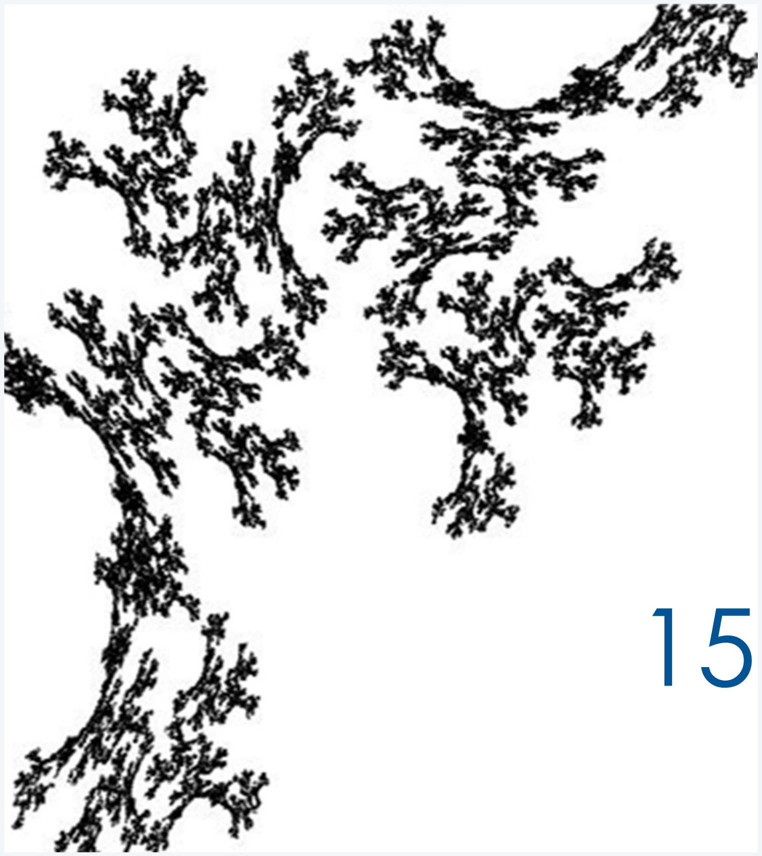
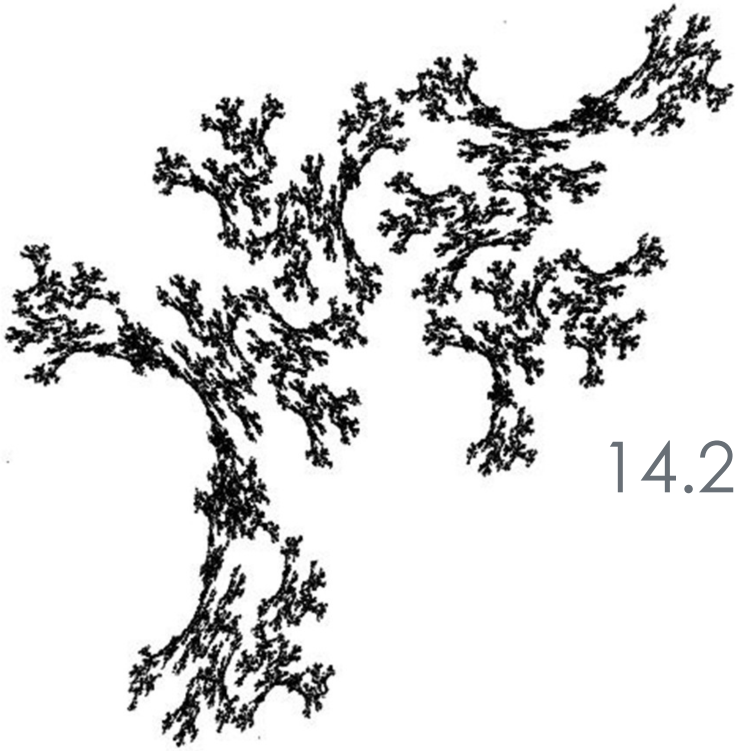


INTRODUCTION TO
DISCRETE STRUCTURES

15.2 Cryptography and RSA

1.1–1.2



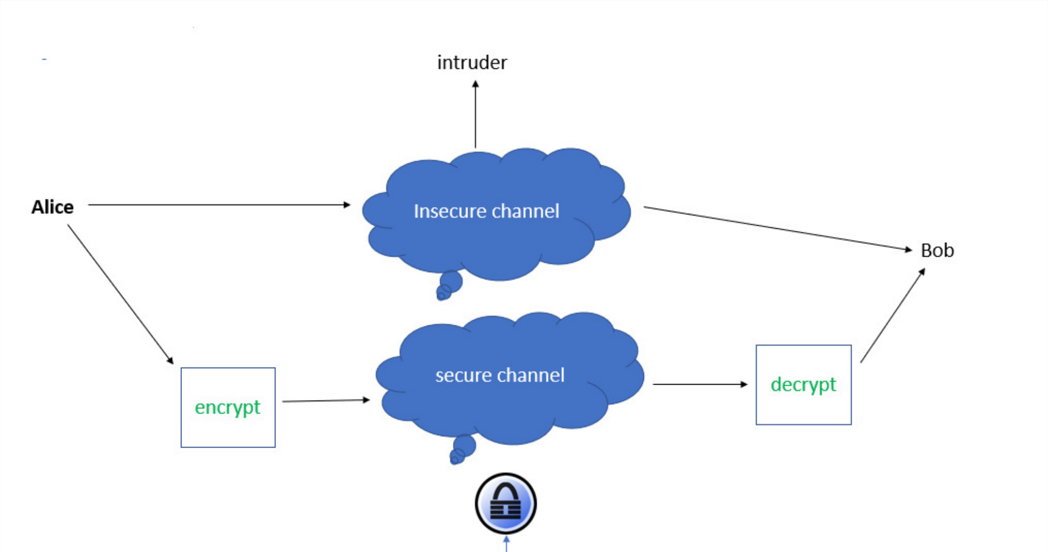
14.2 Cryptography and RSA

- introduction
- ciphers
- RSA algorithm
- Examples of RSA
- Cryptoanalysis

The basic idea

Encryption – change the message in a way that intruder may not decode

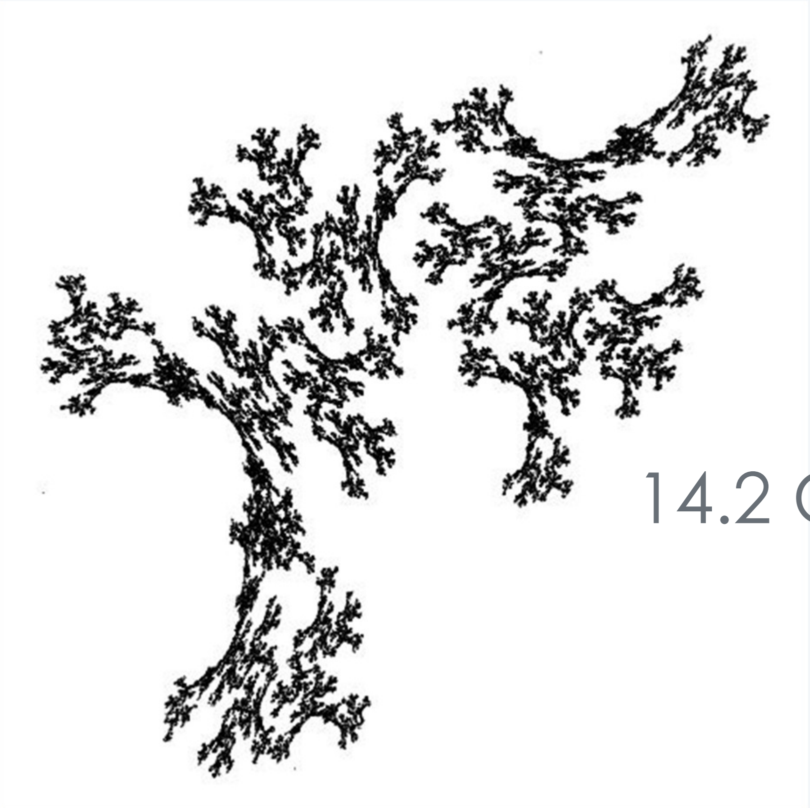
Decryption – use a special key or algorithm to recover the original message.



Quiz

What are some areas of applications of encryption and decryption

1. banking
2. health care
3. ecommerce
4. ???

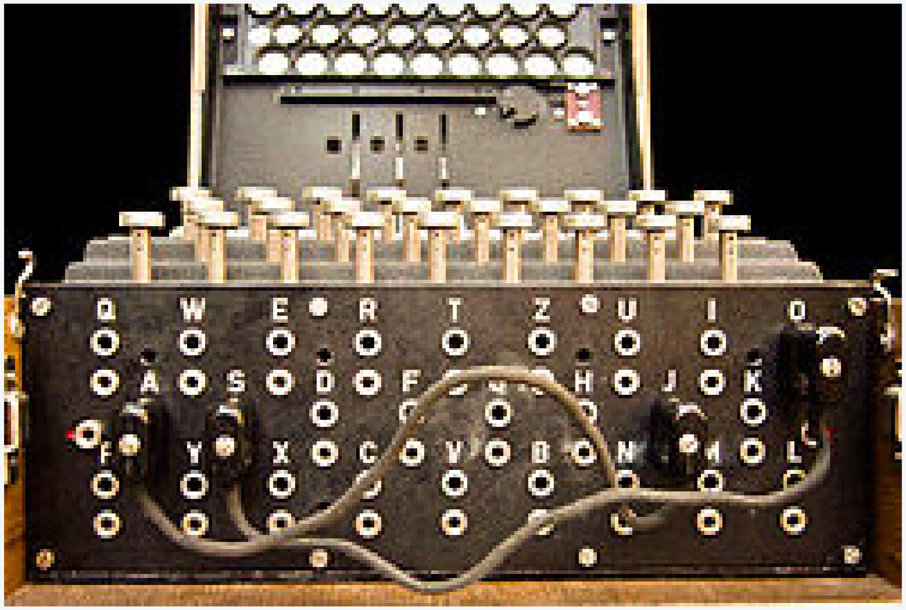


INTRODUCTION TO
DISCRETE STRUCTURES

14.2 Cryptography and RSA

- introduction
- ciphers
- RSA
- Examples of RSA
- Cryptoanalysis

The Enigma machine – World War II German Crypto System



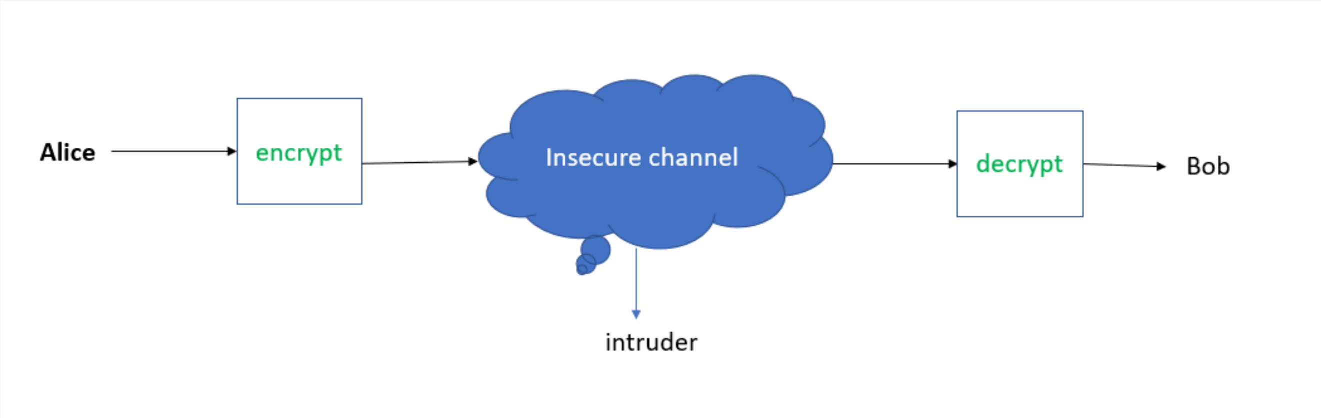
The **Enigma machines** are a series of electro-mechanical rotor cipher machines mainly developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War [source: Wikipedia]

Cryptography - Study of the methods of communication in the presence of adversaries

Cryptography - the basic idea

Alice sends an encrypted message to Bob

Bob uses the decrypted key to read the message



Substitution Cipher (pre-digital era)

The idea.

Substitute letters in the alphabet

Encryption. Replace each letter with a different letter. a ➔ b

Decryption. Inverse the encryption method.

The problem.

Easy to break

Possible attack methods

Frequency analysis

Certain letters and patterns occur more frequently in English (eg: a, e, i, o , u, the, th etc…)

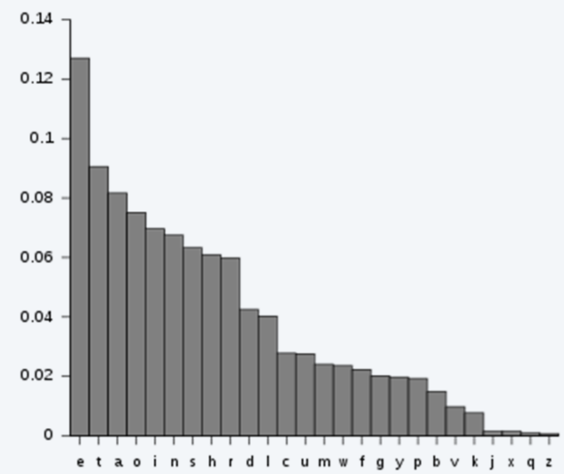
Brute Force

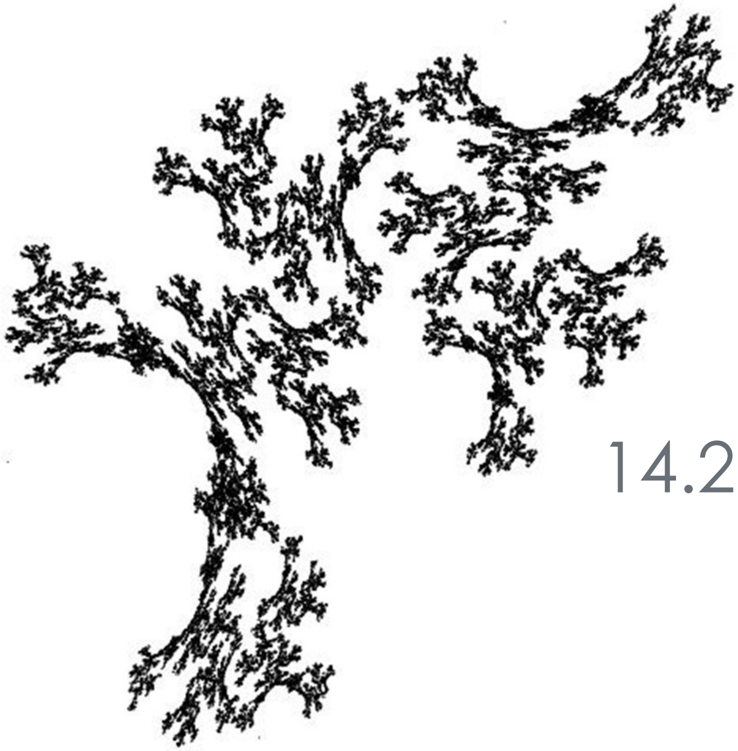
Exhaustive search to break

Question.

How many possible combinations to check? **26!**

26! = 2^{88} operations to find all combinations (really hard)





14.2 Cryptography and RSA

- introduction
- ciphers
- RSA algorithm
- Examples of RSA
- Cryptoanalysis

Advanced Crypto methods

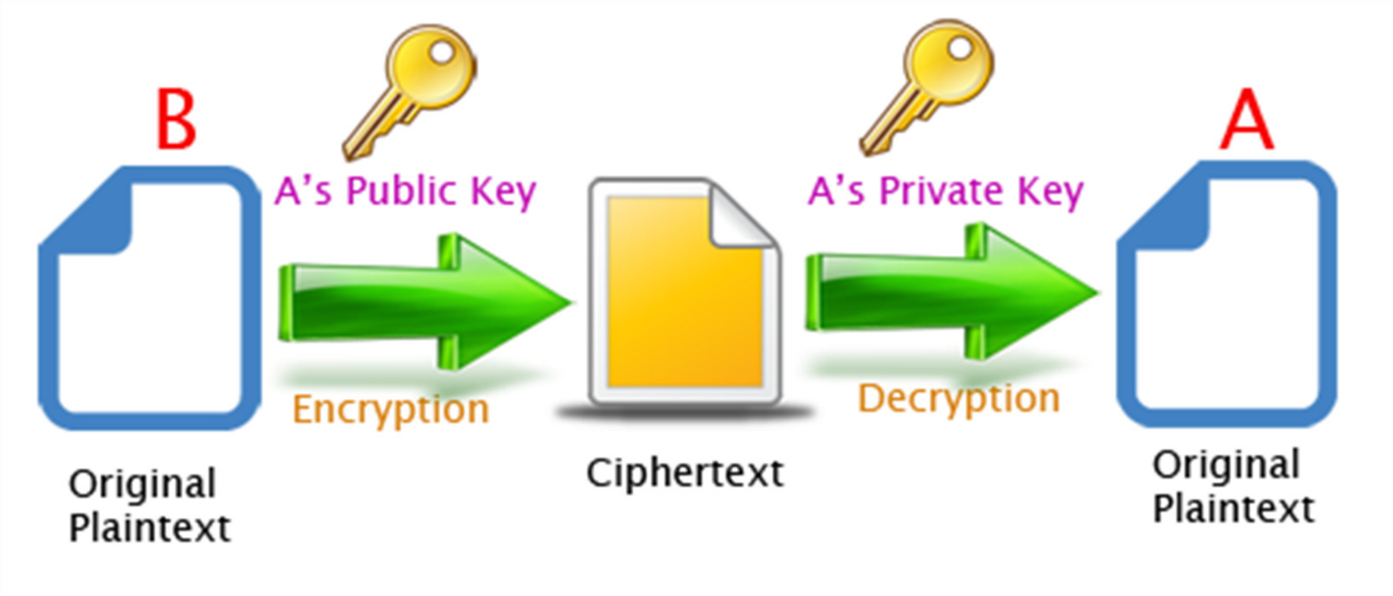
RSA Motivation

Create an “unbreakable” combination of private-public key pairs

A person may own

public key – given to anyone who wants to send a secure message

private key – held privately and used to decrypt messages received.



How RSA (Rivest–Shamir–Adleman **)** works

the **receiver** has both a private key, which they guard closely, and a public key, which they distribute as widely as possible.

A **sender** wishing to transmit a secret message to the receiver encrypts their message using the receiver's widely-distributed public key.

The **receiver** can then decrypt the received message using their closely-held private key

The algorithm

1. Generate two distinct primes, p and q. These are used to generate the private key, and they must be kept hidden. (In current practice, p and q are chosen to be hundreds of digits long.)
2. Let $n ::= pq$.
3. Select an integer $e \in [1, n)$ such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute $d \in [1, n)$ such that $de \equiv 1 \pmod{(p-1)(q-1)}$. This can be done using the Pulverizer.
   The *private key* is the pair (d, n). This should be kept hidden!

How to find (e, n) and (d, n)

Let p=5, q=7

1. Generate two distinct primes, p and q. These are used to generate the private key, and they must be kept hidden. (In current practice, p and q are chosen to be hundreds of digits long.)
2. Let $n ::= pq$.
3. Select an integer $e \in [1, n)$ such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute $d \in [1, n)$ such that $de \equiv 1 \pmod{(p-1)(q-1)}$. This can be done using the Pulverizer.
   The *private key* is the pair (d, n). This should be kept hidden!

Encoding and Decoding process

Encoding To transmit a message $m \in [0, n)$ to **Receiver**, a **Sender** uses the public key to encrypt m into a numerical message

$$m^* ::= \text{rem}(m^e, n).$$

The **Sender** can then publicly transmit m^* to the **Receiver**.

Decoding The **Receiver** decrypts message m^* back to message m using the private key:

$$m = \text{rem}((m^*)^d, n).$$

Examples.

Let n = 35

(e, n) = (11, 35)

(d, n) = (11, 35)

Show that message 2 can be encrypted with e and decrypted with d

Can we break RSA?

Is it easy to find the prime factorization of integers?

The RSA-2048 (n is 2048 bits long) Challenge Problem would take 1 billion years with a classical computer. "A quantum computer could do it in 100 seconds?"

Questions

1. Are there infinite number of primes?

Proof.

2. What is the largest prime number known?

The **largest** known **prime number** (as of August 2019) is $2^{82,589,933} - 1$, a **number** which has 24,862,048 digits when written in base 10 [source: Wikipedia]

Exercise. (challenge) Show that given just the private and the public keys, it is easy to factor n

Can we break RSA?

How many primes are below n? (by Gauss in 18th century)

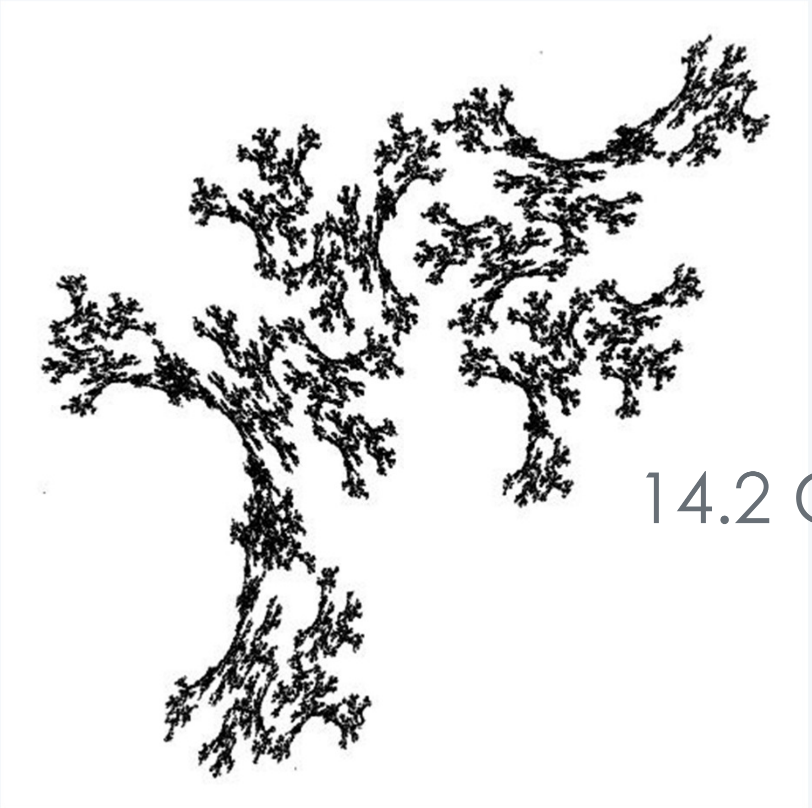
$$\pi(n) \sim \frac{n}{\log n},$$

Cost of computing

It is easy to verify that product of two given primes is equal to n. Just multiply the two prime numbers. Of course, it would take some time, if the product is greater than the max int that can fit in a computer.

But why is it extremely difficult to compute p and q, given n = p.q

Proof.



14.2 Cryptography and RSA

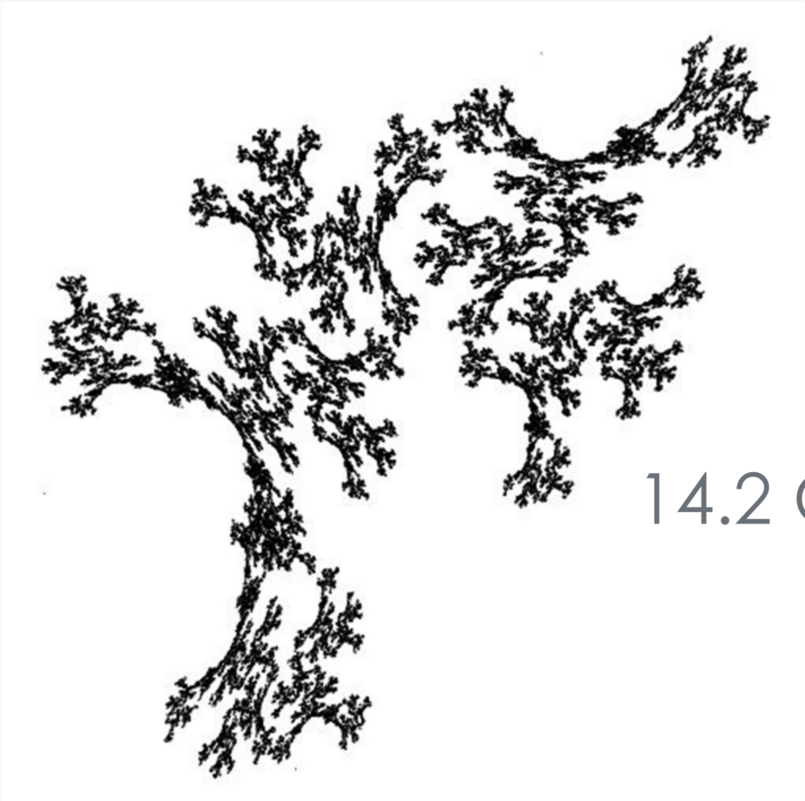
- introduction
- ciphers
- RSA algorithm
- Examples of RSA
- Cryptoanalysis

workshop

Given two primes 3 and 5, generate public and private key pairs. Encrypt and decrypt the message 2

workshop

Given two primes 5 and 7, generate public and private key pairs. Encrypt and decrypt the message 2



14.2 Cryptography and RSA

- introduction
- ciphers
- RSA algorithm
- Examples of RSA
- Cryptoanalysis

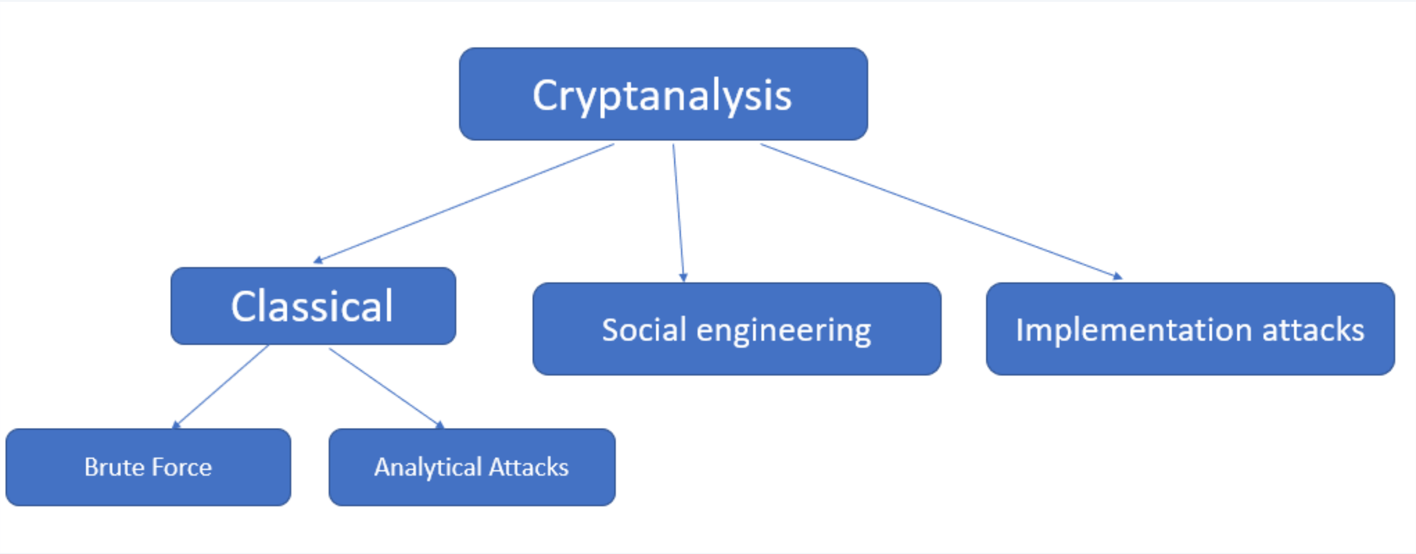
Cryptoanalysis – The study of the breaking of the code

There are number of ways that encryption can be attacked.

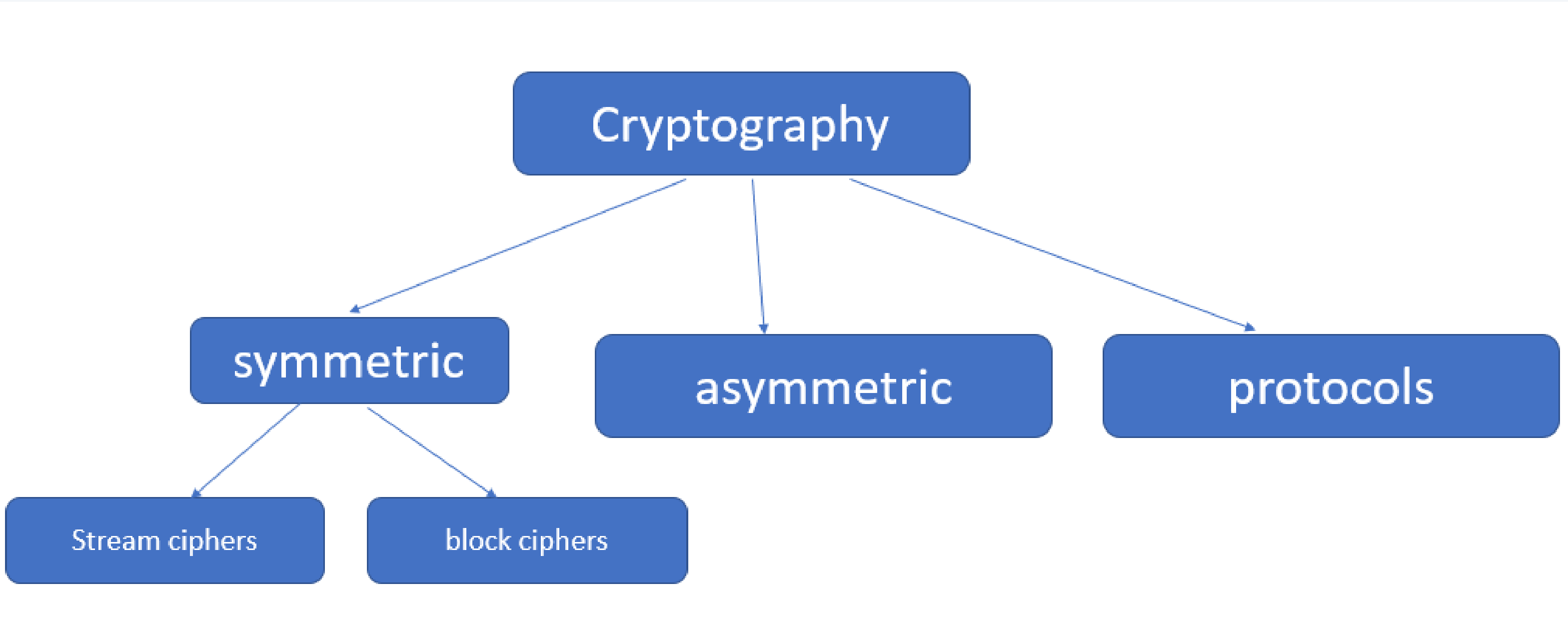
Classical attacks – uses brute force of analytical attacks

Social Engineering – uses psychological manipulation of people

Implementation attacks. Exploit vulnerabilities in the implementation



Crypto Tree



Cryptography - the art of writing or solving codes.

Symmetric cryptography – uses the same key for encryption and decryption

Asymmetric cryptography – uses different keys for encryption and decryption

Cryptographic protocols - performs a security-related function and applies cryptographic methods

INTRODUCTION TO
DISCRETE STRUCTURES

14.2 Cryptography and RSA

- introduction
- ciphers
- RSA algorithm
- Examples of RSA
- Cryptoanalysis

INTRODUCTION TO DISCRETE STRUCTURES

15.2 Cryptography and RSA

1.1–1.2