Cryptography

Classification of Cryptography

Symmetric Key Cryptography

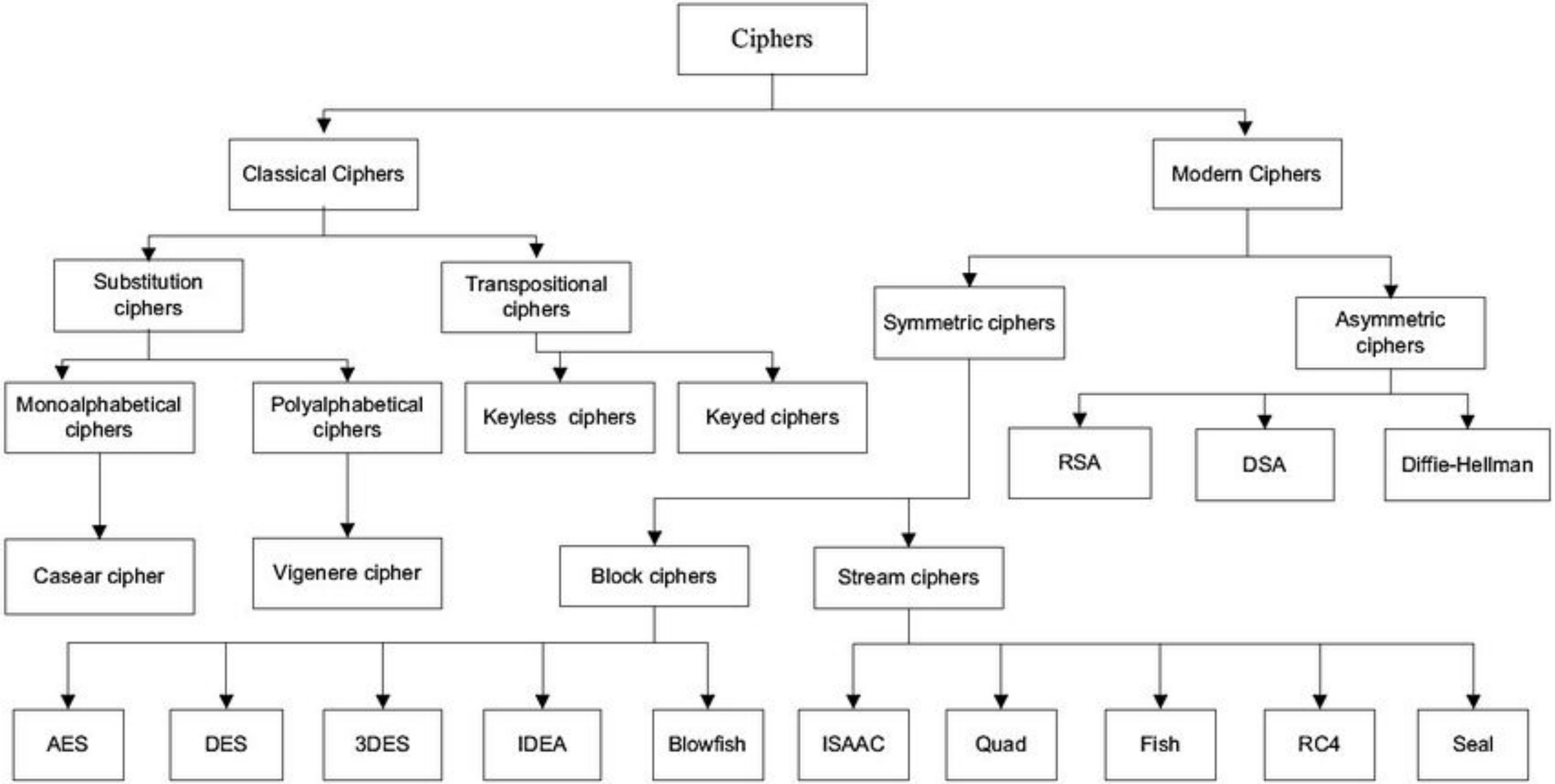
M S Vilkhu

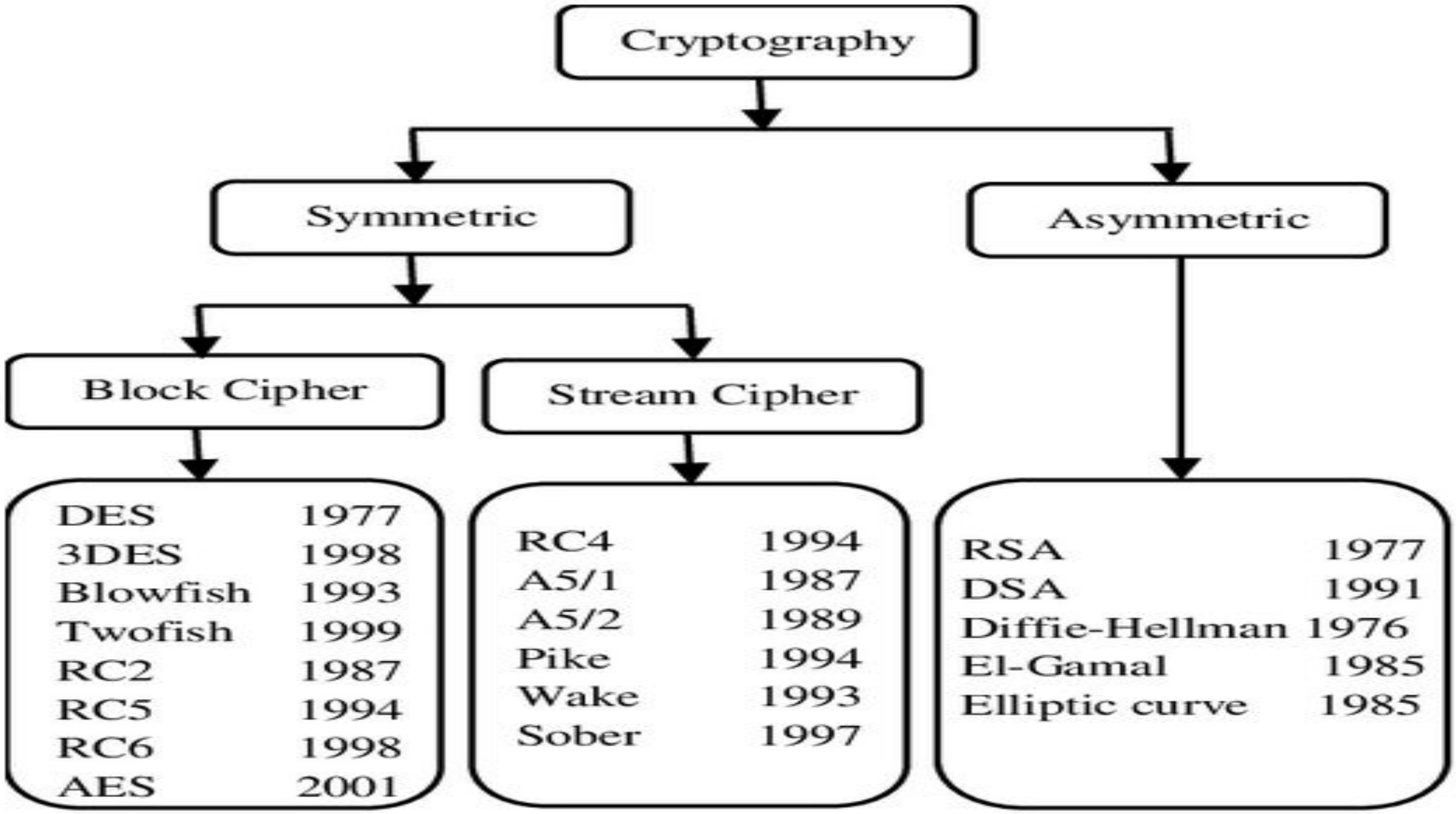
14 Sep 2024

Learning Objectives

- Classification of Cryptography
- overview of the main concepts of **symmetric cryptography**.
- **difference** between **cryptanalysis** and **brute-force attack**.
- Understand the operation of a **monoalphabetic substitution cipher.**
- Understand the operation of a **polyalphabetic** cipher.
- Present an overview of the **Hill cipher**.
- Describe the of a rotor machine.

Classification





Cryptography

Symmetric

Asymmetric

Block Cipher

Stream Cipher

DES	1977
3DES	1998
Blowfish	1993
Twofish	1999
RC2	1987
RC5	1994
RC6	1998
AES	2001

RC4	1994
A5/1	1987
A5/2	1989
Pike	1994
Wake	1993
Sober	1997

RSA	1977
DSA	1991
Diffie-Hellman	1976
El-Gamal	1985
Elliptic curve	1985

Cryptographic Algorithms Classification

Cryptography classified along 3 independent dimensions

- Cryptographic systems classified along **3 independent dimensions**:

1. **Type of operations used for transforming plain text to cipher text**

- All the **encryption algorithms** are based on **two general principles**:
  - **substitution**, in which each element in the plaintext is **mapped into another** element, and
  - **transposition**, in which elements in the plaintext are **rearranged**.

2. **The number of keys used**

- If the sender and receiver uses same key then it is said to be **symmetric key (or) single** key (or) conventional encryption.
- If the sender and receiver use different keys then it is said to be **public key encryption**.

3. **The way in which the plain text is processed**

- A **block cipher** processes the input and **block of elements at a time**, producing output block for each input block.
- A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

3 categories of encryption

- most encryption techniques **fall into one of three main categories**: symmetric cryptography algorithms, asymmetric cryptography algorithms or hash functions.

- Although hybrid systems do exist (such as the SSL internet protocols)

1. **Symmetric key cryptography**
2. **Asymmetric key cryptography**
3. **One-way hash algorithms**

This is the classification which will referred and studies

3 categories of encryption

1. Symmetric key cryptography

- Also known as **private key cryptography**, **secret key cryptography** or **single-key encryption**,
- symmetric key encryption **uses only one key** for both the **encryption process and decryption process.**
- For these types of systems, **each user must have access to the same private key**.
- Private keys might be **shared either through a previously established secure communication channel**
  - like a private courier or
  - secured line or,
  - more practically, a secure key exchange method like the Diffie-Hellman key agreement.

3 categories of encryption

1. Symmetric key cryptography

- **2 types** of **symmetric key** algorithms:
- **Block cipher**: In a block cipher, the cipher algorithm works on a **fixed-size block of data**. For example, if the block size is eight, eight bytes of plaintext are encrypted at a time. Normally, the user's interface to the encrypt/decrypt operation handles data longer than the block size by **repeatedly calling the low-level cipher function**.
- **Stream cipher**: Stream ciphers do not work on a block basis, but rather **convert one bit (or one byte) of data at a time**.
- Basically, a stream cipher generates a **keystream** based on the **provided key**.
- The generated **keystream** is then **XORed** with the **plaintext data**.

3 categories of encryption

1. Symmetric key cryptography

- **Examples of symmetrical cryptography**:
- **Data Encryption Standard (DES)**:
- The Data Encryption Standard (DES) was developed by IBM in the early 1970's, and while it is now considered to be susceptible to brute force attacks, its architecture remains highly **influential** in the field of modern cryptography.
- **Triple DES**: While advancements in computing made **DES insecure by 1999**, the DES cryptosystem built on the original DES foundation adds t**extra levels of security** hat cannot be broken by modern machines.
- **Blowfish**: A fast, free, publicly available **block cipher** designed by **Bruce Schneer in 1993**.
- **Advanced Encryption Standard (AES)**: The Advanced Encryption Standard (AES) is the first and only **publicly accessible** cipher that is approved by the US National Security Agency for **top secret information**.

3 categories of encryption

2. Asymmetric key cryptography

- In asymmetric encryption, a **pair of keys** is used:
  - one secret key and
  - one public key.
- For this reason, these algorithms are also referred to **as public key algorithms**.

- **Public key cryptography** is considered to be **more secure** than symmetric encryption techniques because even though one key is publicly available, an encrypted message can only be decrypted with the intended **recipient's private key**.

3 categories of encryption

2. Asymmetric key cryptography

- **examples of asymmetrical cryptography**
- **RSA**: Named for its **founders—Rivest, Shamier and Adleman**—in 1977, the RSA algorithm is one of the oldest **widely used public key** cryptosystems used for **secure data transmission.**
- **ECC**: **Elliptic curve cryptography** is an **advanced form** of asymmetric encryption that uses the **algebraic structures of elliptic curves** to create **strong cryptographic keys**.

3 categories of encryption

3. One-way hash algorithms

- A cryptographic hash algorithm **produces a fixed-length output string** (often called a **digest**) from a **variable-length input string**.
- The **input** serves as the **plaintext**, and the **output** hash is the **cipher**.

- For all practical purposes, the following statements **are true of a good hash function**:

  - **Collision resistant**: If **any portion** of the data is **modified**, a **different hash** is generated, ensuring **data integrity**.

  - **One-way**: The function is **irreversible**. That is, given a digest, it is not possible to find the data that produces it, **ensuring data security.**

3 categories of encryption

3. One-way hash algorithms

- **hash algorithms** make for **effective cryptosystems** because the hash algorithm **encrypts the data directly** without the need for different keys. In essence, the plaintext is its own key.
- Consider the security vulnerability of a database of stored bank account passwords. Anyone with either authorized or unauthorized access to the bank's computer systems might **potentially read every password.**
- To maintain data security, banks and other businesses **encrypt sensitive information like passwords into a hash value** and store only that encrypted value in their database. Without knowing the user's password,
- the hash value cannot be broken.

Thank You