CS 6530 Applied Cryptography

July-Nov 2025

Introduction to Cryptography and Data Security

29th July 2025

Dr. Manikantan Srinivasan

(Material covered is based on Chapter 1 of

Understanding Cryptography – Second Edition

Courtesy: Slides by Authors - Christof Paar and Jan Pelzl)

Contents of Chapter 1

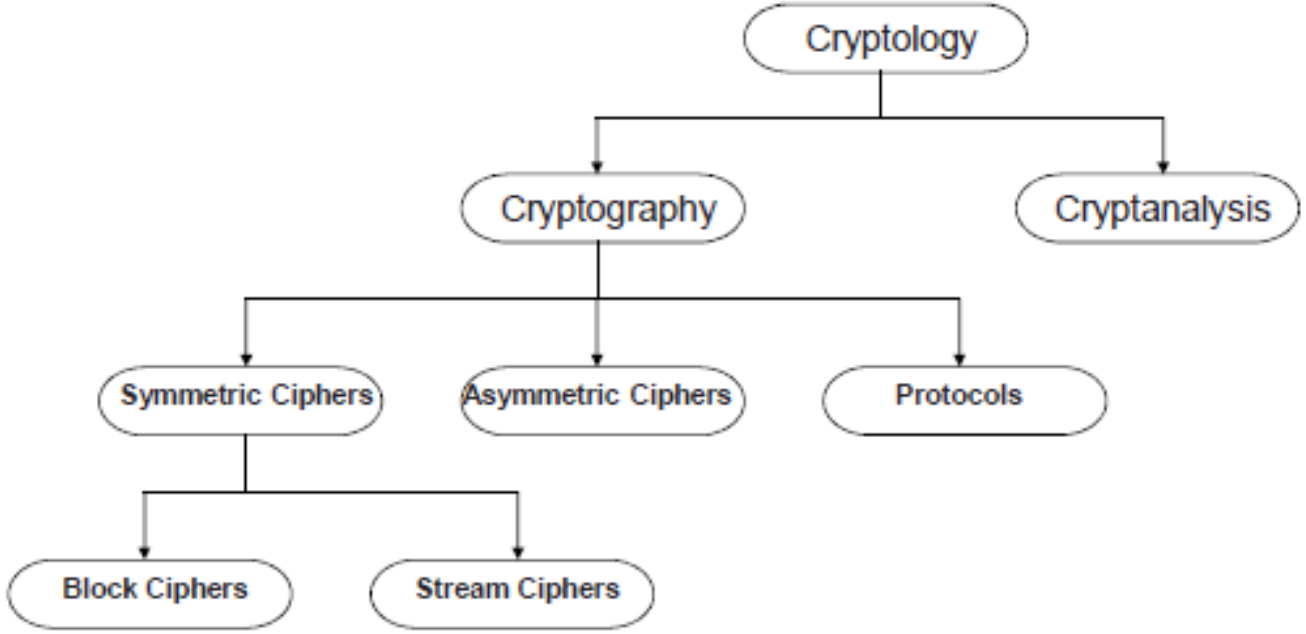
- **Overview on the field of cryptology**
- Basics of symmetric cryptography
- Cryptanalysis
- Substitution Cipher
- Modular arithmetic
- Shift (or Caesar) Cipher and Affine Cipher

Further Reading and Information (As per Authors of BooK UC)

- **Addition to *Understanding Cryptography* .**
  - A.Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, October 1996.
  - H.v.Tilborg (ed.), *Encyclopedia of Cryptography and Security*, Springer, 2005
- **History of Cryptography (great bedtime reading)**
  - S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor, 2000.
  - D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. 2nd edition, Scribner, 1996.
- **Software (excellent demonstration of many ancient and modern ciphers)**
  - *Cryptool, http://www.cryptool.de*

Classification of the Field of Cryptology

- Cryptography is the science of securing communication against the adversary. Main aim is to hide the message. Now used for Integrity and authenticity as well.
- Cryptanalysis is the science and sometimes art of *breaking* cryptosystems.
- Symmetric Algorithms: Two parties have an encryption and decryption method for which they share a secret key. (Until 1976, were symmetric. Still widely used)

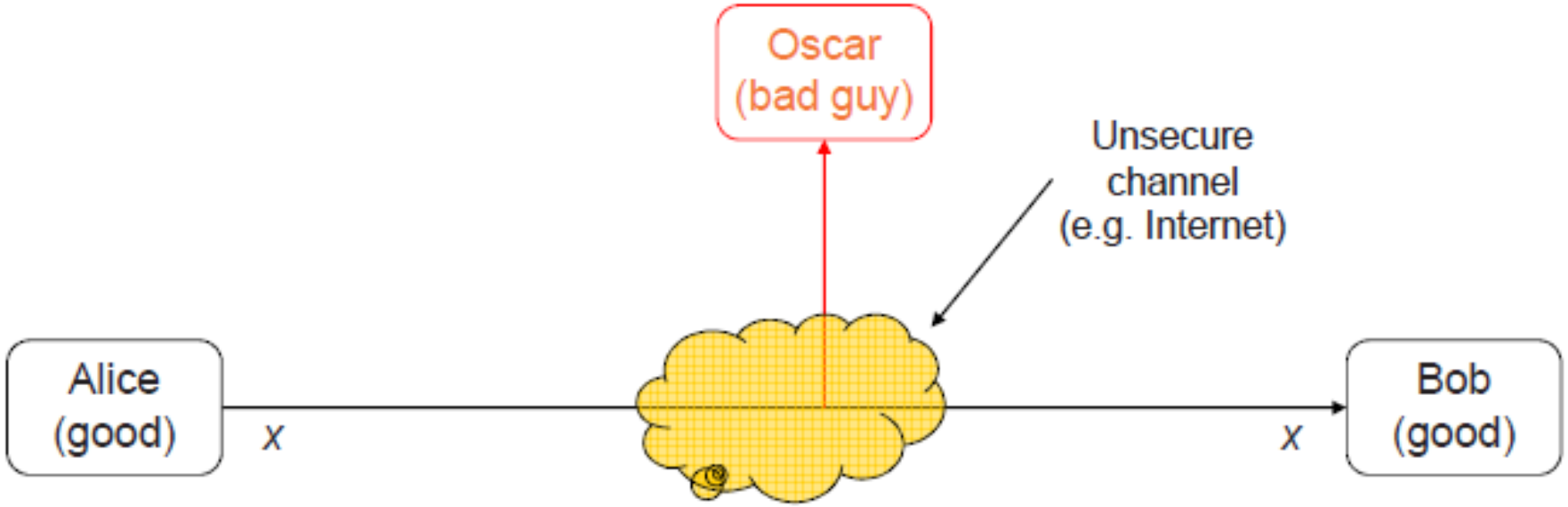


- Asymmetric (or Public-Key) Algorithms: Whitfield Diffie, Martin Hellman, Ralph Merkle introduced new type of cipher: In Public-Key cryptography, two keys exist: User has a Secret key, as well as a public key.
- Cryptographic Protocols: They realize more complex security functions through the use of cryptographic algorithms. TLS (Transport Layer Security) is an example.
  - Most protocols use Hybrid schemes : symmteric ciphers (e.g., for encryption and message authentication) and • asymmetric ciphers (e.g., for key exchange and digital signature).

Basics of Symmetric Cryptography

Symmetric Cryptography

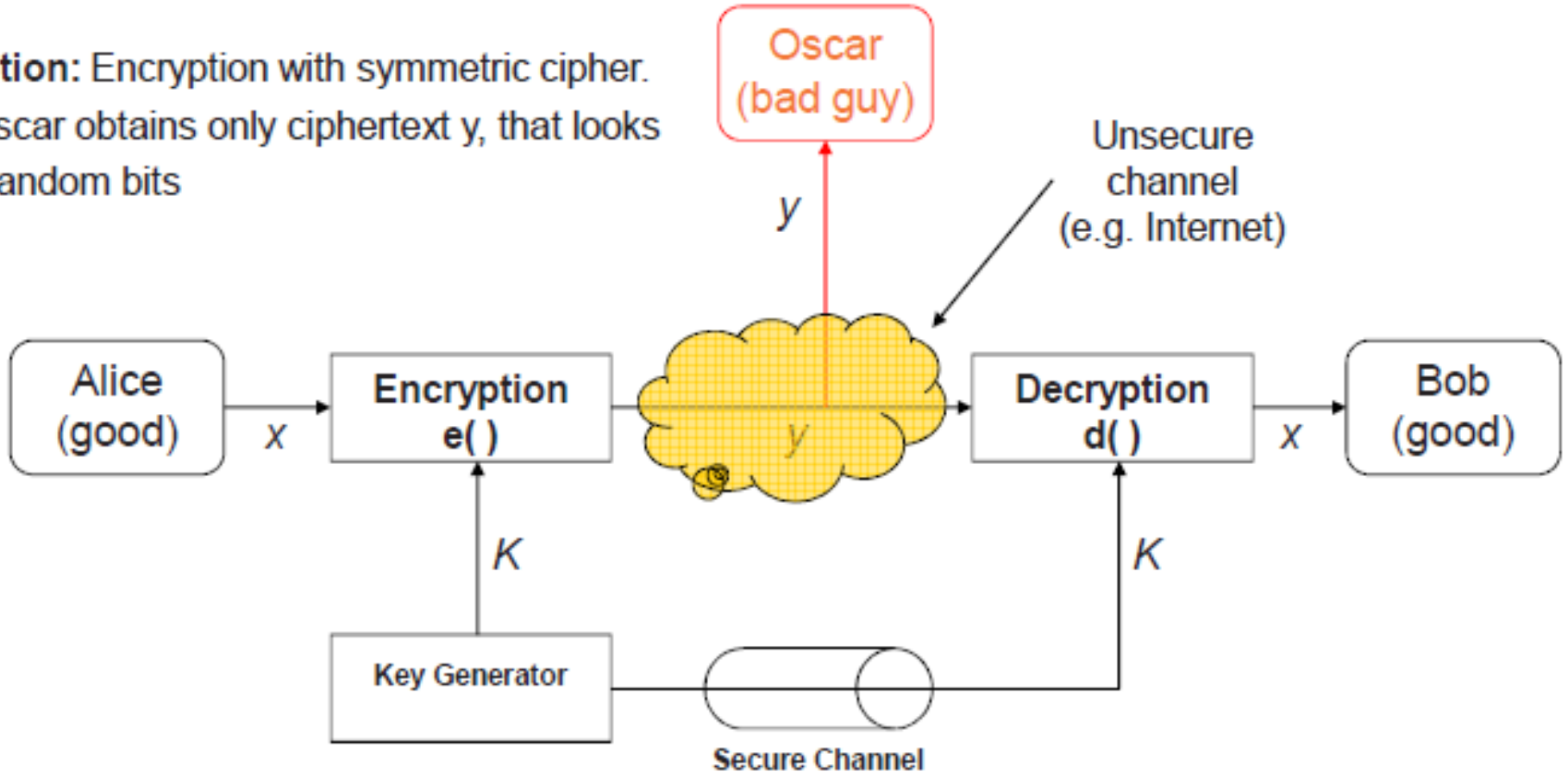
- Alternative names: **private-key**, **single-key** or **secret-key** cryptography.



- **Problem Statement:**
  1) Alice and Bob would like to communicate via an unsecure channel (e.g., WLAN or Internet).
  2) A malicious third party Oscar (the bad guy) has channel access but should not be able to understand the communication.

Symmetric Cryptography

Solution: Encryption with symmetric cipher.
⇒ Oscar obtains only ciphertext y, that looks like random bits



- x is the. **plaintext**
- y is the **ciphertext**
- *K* is the **key**
- Set of all keys {*K*1, *K*2, ...,*Kn*} is the **key space**

Symmetric Cryptography

- Encryption equation $y = e_K(x)$
- Decryption equation $x = d_K(y)$

- Encryption and decryption are inverse operations if the same key K is used on both sides:

$$d_K(y) = d_K(e_K(x)) = x$$

- Important: The key must be transmitted via a **secure channel** between Alice and Bob.
- The secure channel can be realized, e.g., by manually installing the key for the Wi-Fi Protected Access (WPA) protocol or a human courier.
- However, the system is only secure if an attacker does not learn the key K!

⇒ **The problem of secure communication is reduced to secure transmission and storage of the key K.**

Attacking crypto schemes

Why do we need Cryptanalysis

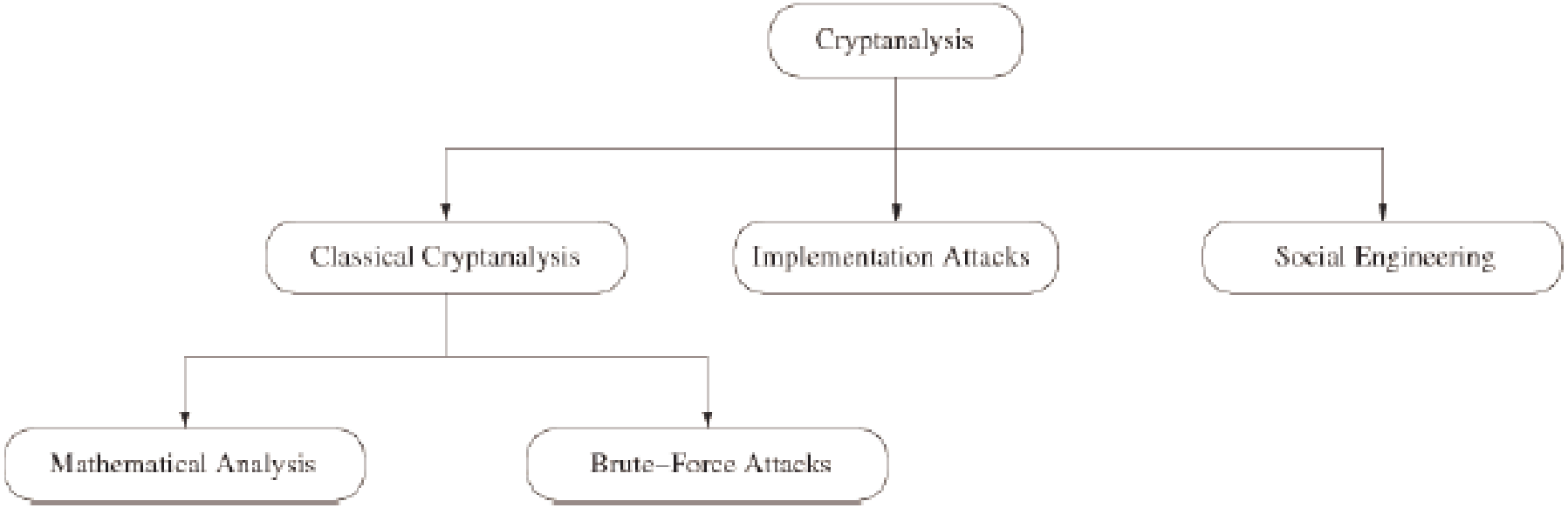
- There is no *mathematical proof of security* for any practial cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail) !

Kerckhoff's Principle is paramount in modern cryptography:

> A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key.

- In order to achieve Kerckhoff's Principle in practice:
  Only use widely known ciphers that have been cryptanalyzed for several years by good cryptographers! (*Understanding Cryptography* only treats such ciphers)
- **Remark:** It is tempting to assume that a cipher is „more secure" if its details are kept secret. However, history has shown time and again that secret ciphers can almost always been broken once they have been reversed engineered. (Example: Content Scrambling System (CSS) for DVD content protection.)

Cryptanalysis: Attacking Cryptosystems



- **Classical Attacks**
  - Mathematical Analysis
  - Brute-Force Attack
- **Implementation Attack**: Try to extract key through reverese engineering or power measurement, e.g., for a banking smart card.
- **Social Engineering**: E.g., trick a user into giving up her password

Brute-Force Attack (or Exhaustive Key Search) against Symmetric Ciphers

- Treats the cipher as a black box
- Requires (at least) 1 plaintext-ciphertext pair (x_0, y_0)
- Check all possible keys until condition is fulfilled:

$$d_K(y_0) \stackrel{?}{=} x_0$$

- How many keys to we need ?

Key length in bit	Key space	Security life time (assuming brute-force as best possible attack)
64	2^{64}	**Short term** (few days or less)
128	2^{128}	**Long-term** (several decades in the absence of quantum computers)
256	2^{256}	**Long-term** (also resistant against quantum computers – note that QC do not exist at the moment and might never exist)

Important: An adversary only needs to succeed with **one** attack. Thus, a long key space does not help if other attacks (e.g., social engineering) are possible..

Substitution Cipher

Substitution Cipher

- Historical cipher
- Great tool for understanding brute-force vs. analytical attacks
- Encrypts letters rather than bits (like all ciphers until after WW II)

Idea: replace each plaintext letter by a fixed other letter.

Plaintext		Ciphertext
A	→	k
B	→	d
C	→	w
	....	

for instance, ABBA would be encrypted as kddk

- Example (ciphertext):

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb  hcc
                hwwhbsqvqbre hwq vhlq
```

- How secure is the Substitution Cipher? Let's look at attacks…

1. Attack: Exhaustive Key Search (Brute-Force Attack)

- Simply try every possible subsititution table until an intelligent plaintext appears (note that each substitution table is a key)..
- How many substitution tables (= keys) are there?

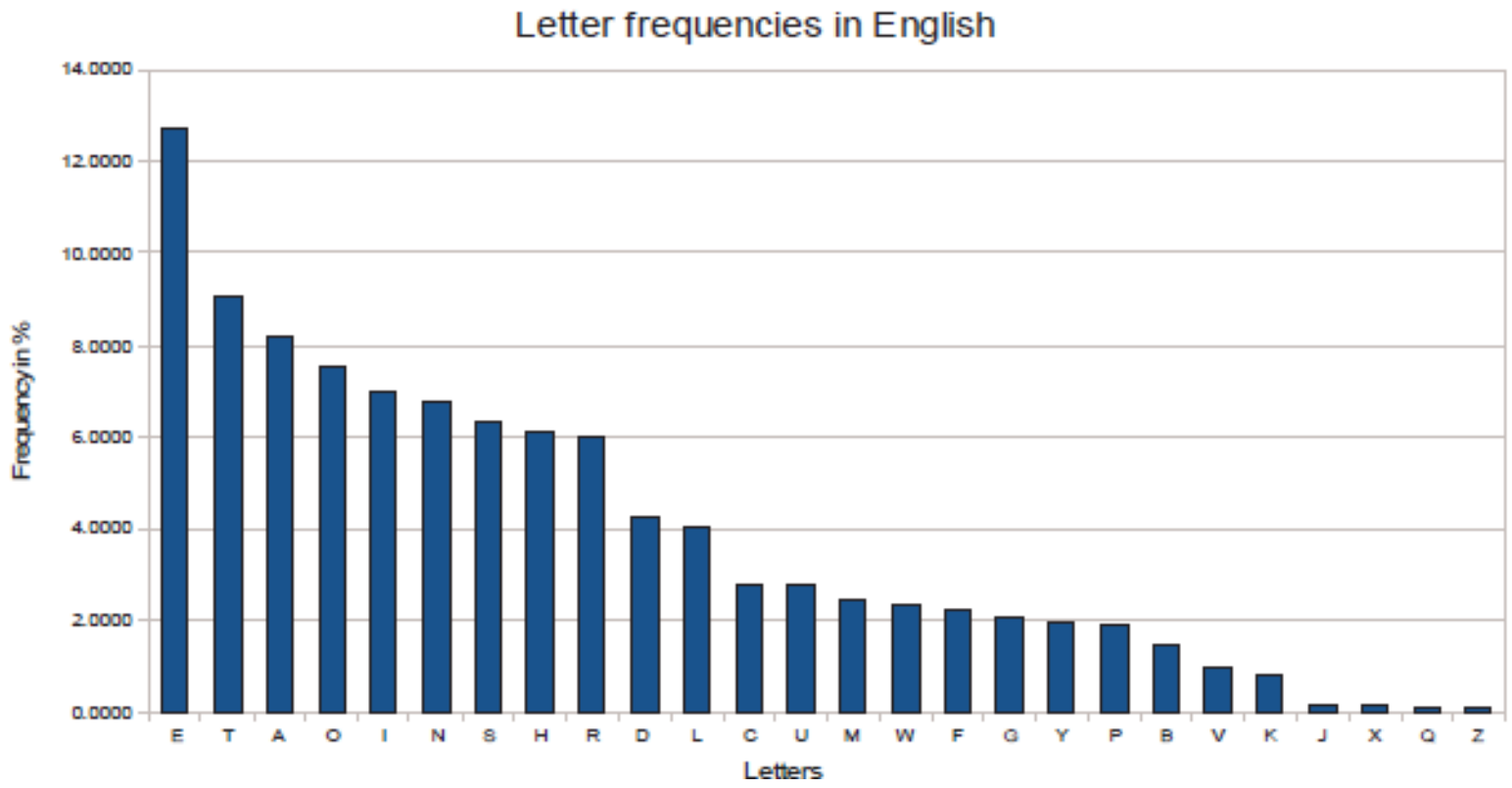
$$26 \times 25 \times \ldots \times 3 \times 2 \times 1 = 26! \approx 2^{88}$$

Search through 2^{88} keys is completely infeasible with today's computers!
(cf. earlier table on key lengths)

- Q: Can we now conclude that the substitution cipher is secure since a brute-forece attack is not feasible?
- A: No! We have to protect against **all** possible attacks…

2. Attack: Letter Frequency Analysis (Brute-Force Attack)

- Letters have very different frequencies in the English language
- Moreover: the frequency of plaintext letters is preserved in the ciphertext.
- For instanc, „e“ is the most common letter in English; almost 13% of all letters in a typical English text are „e“.
- The next most common one is „t“ with about 9%.



Breaking the Substitution Cipher with Letter Frequency Attack

- Let's retun to our example and identify the most frequent letter:

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb hcc
hwwhbsqvqbre hwq vhlq
```

- We replace the ciphertext letter `q` by `E` and obtain:

```
iE ifcc vEEr fb rdE vfllcE na rdE cfjwhwz hr bnnb  hcc
hwwhbsEvEbre hwE vhlE
```

- By further guessing based on the frequency of the remaining letters we obtain the plaintext:

```
WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL
ARRANGEMENTS ARE MADE
```

Breaking the Substitution Cipher with Letter Frequency Attack

- In practice, not only frequencies of individual letters can be used for an attack, but also the frequency of letter pairs (i.e., „th“ is very common in English), letter triples, etc.
- cf. Problem 1.1 in *Understanding Cryptography* for a longer ciphertext you can try to break!

Important lesson: Even though the substitution cipher has a sufficiently large key space of appr. 2^{88}, it can easily be defeated with analytical methods. This is an excellent example that an encryption scheme must withstand all types of attacks.

Thank you – Q&A