Information Security
(WBCS004-05)

Fatih Turkmen

Office: 0420 (Please schedule first through email)

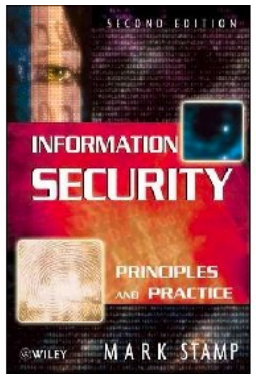
Some slides are borrowed from Dr. Frank B. Brokken and Dr. Suman Jana

Today

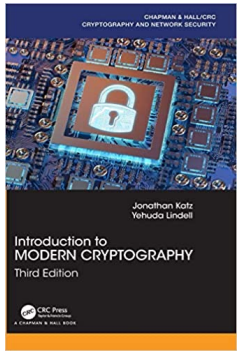
- First things first: **Logistics/Organization**
- Then
  - Introduction to Information Security
  - Crypto Basics:
    - Ceasar's Cipher,
    - Vigenere Cipher,
    - (Generalized) Substitution Ciphers
    - Transposition Cipher
  - Cryptanalysis

Books

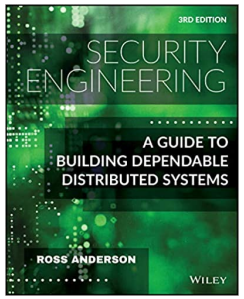
- **Information Security: Principles and Practice, 2nd Edition, 2011**



- Introduction to Modern Cryptography, Third Edition



- Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition



Topic overview

Week	Topic	
1	Introduction + Information Security	
2	Cryptography 1 (Symmetric)	
3	Cryptography 2 (Asymmetric)	
4	Access Control	Fadi Mohsen
5	Cryptography 3 (Hashing)	
6	Protocols	Fadi Mohsen
7	Privacy	
8	Software Security or PGP Practical (GPG) or Side Channels or Advanced Crypto	→ TBD

TAs and Communication

- Lars Andringa
- Lorenzo Rota
- Pooja Gowda

- **BS** is where the Course Material will be stored and important announcements are made.
- **Discussion groups** for general questions and forming groups.
- Questions? mailto: infosec-course@rug.nl

Schedule

Week/Dates	Topic	Published (Wednesday 12:00am)	Deadline (Friday, 23:59pm)	Lab/Tutorial (To be Confirmed)
7.9	Introduction			
14.9	Cryptography 1 (Symmetric)	Assignment 1		Thu (13:00 - 15:00) Fri (11:00 - 13:00)
21.9	Cryptography 2 (Asymmetric)	Assignment 2	Assignment 1	Thu (13:00 - 15:00) Fri (11:00 - 13:00)
28.9	Access Control	Assignment 3	Assignment 2	Thu (13:00 - 15:00) Fri (11:00 - 13:00)
5.10	Cryptography 3 (Hashing)		Assignment 3	
12.10	Protocols	Assignment 4		Thu (13:00 - 15:00) Fri (11:00 - 13:00)
19.10	Privacy			Thu (13:00 - 15:00) Fri (11:00 - 13:00)
26.10	Software Security or PGP Practical (GPG)		Assignment 4	

Practical Assignments

- Goal: **to gain basic understanding of security and privacy by analysis and construction of theoretical concepts**

- Four (4) practical assignments
  - Content, information and deadlines **on BS**
  - No intermediate feedback!

- You will work in **groups of two or three**
  - Create groups both on BS (for grading purposes) and Themis

8

Assignment delivery

- Reports + code to **themis.housing.rug.nl**
- Solutions are to be uploaded on time
- Grading penalties apply:
  - No delivery: **100%**
  - Unacceptable delivery: **100%**
  - Irregular delivery (possible): **50%**

9

Assignment delivery (cont.)

- What constitutes an *unacceptable* delivery?
  - Delivery **after** the deadline
  - **Plagiarism** of another student's answers (penalty applies to **all students involved**, disputes to be resolved by BoE)
  - **Copy/paste** from an online repository
    - Minor modifications are not accepted
    - If you inspire from a Web site, explain how you "significantly" differ from that with an additional note.
  - The submission is **unreadable** (e.g., a failing PDF)
  - The submission documents contain any items that are **scanned from notes or photographed**, e.g., no handwritten solutions will be accepted

10

Assignment delivery (cont.)

- What constitutes *irregular* delivery?
  - The files are sent by email, delayed due to miscommunication, etc.
  - Proof that the assignment was **finalized** before the deadline is required
  - Lecturers and TAs decide on acceptability

11

Corner cases

- Assignment grades can be retained for the next year max
  - **Repeating students** from last year mail us **ASAP** for the retention of grades

- Follow the rules in the Communication section of BS diligently

12

Grading

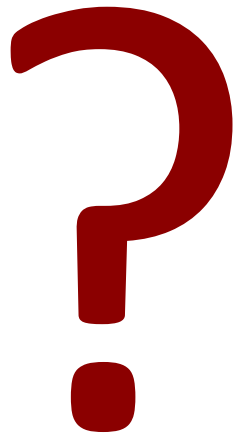
- Practical Assignments (A)
- Written Exam (E)

Final Grade (F)

```
if (A >= 5.0 and E >= 5.0) then
        F=(.6*A + .4*E)
else
        otherwise (A<5 or E<5) F=min(A,E)
```

- 6.0 is still the minimum for passing grade
- Round >*.25 and >*.75 up except for (5.25, 6) -> 6

Questions about the organization?



14

What is Information Security?

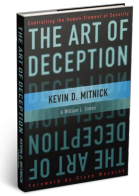
The practice of protecting information by mitigating information risks.

What is Information Security? (cont.)

What is it really in practice?

- A race between an attacker and defender?

- The “Art of Deception” [cf: Kevin Mitnick]?



- A yearly conference on ”Ethical Hacking” (i.e., hackathon)?

- …?

Different Perspectives – 1

- The art of adversarial thinking

“Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.”

- Bruce Schneier

Different Perspectives – 2

- Good Defense with Lessons Learned

- The Stronghold of Bourtange
  - Defense in depth
  - Variation of Defenses
  - A limited number of ports of entry
  - A sentry who knows his/her stuff at critical points

Where is this?

Information Security: Objectives

- CIA

Information Security: Aims

- CIA
  - Confidentiality
    - unauthorized *reading* of information

Information Security: Aims

- CIA
  - Confidentiality
    - unauthorized *reading* of information
  - Integrity
    - unauthorized *writing/modification* of information

Information Security: Aims

- CIA
  - Confidentiality
    - unauthorized *reading* of information
  - Integrity
    - unauthorized *writing/modification* of information
  - Availability
    - The information/service must be available when needed

Risks of Information **In**security

- What are the risks involved when CIA is reduced or neglected?

Risks of Information Insecurity (cont.)

- Confidentiality → Unauthorized Access to:
  - personnel and student records and accounts
  - medical records
  - financial information
  - access information to (computer, bank) accounts
  - e-mail
  - student progress data

Risks of Information Insecurity (cont.)

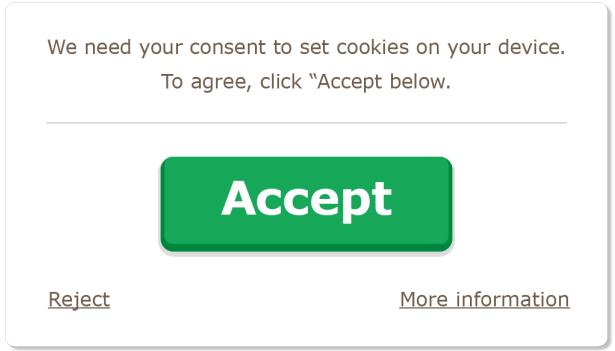
- Integrity → Compromising information stored in computers:
    - legal records
    - tax information
    - financial data
    - in general: modifying information considered sensitive, confidential or secret.

Risks of Information **In**security (cont.)

- Availability → Service disruption:
  - resource blocking/stealing
  - slowed down computer or network
  - 3rd party initiated/controlled illegal activities
  - downtime, costly repairs

Legal Basis

- General Data Protection Regulation
  - cf: http://www.eugdpr.org/
  - Aim: protect all EU citizens from privacy and data breaches
    - subjects must have given their consent
    - data may only be used for intended purpose
    - no additional data may be collected
    - integrity, confidentiality are required



What is GDPR?

Legal Basis (cont.)

- EU-US Privacy Shield:

This framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. It allows the free transfer of data to companies that are certified in the US under the Privacy Shield.

May be dead now? Cf: https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/ …

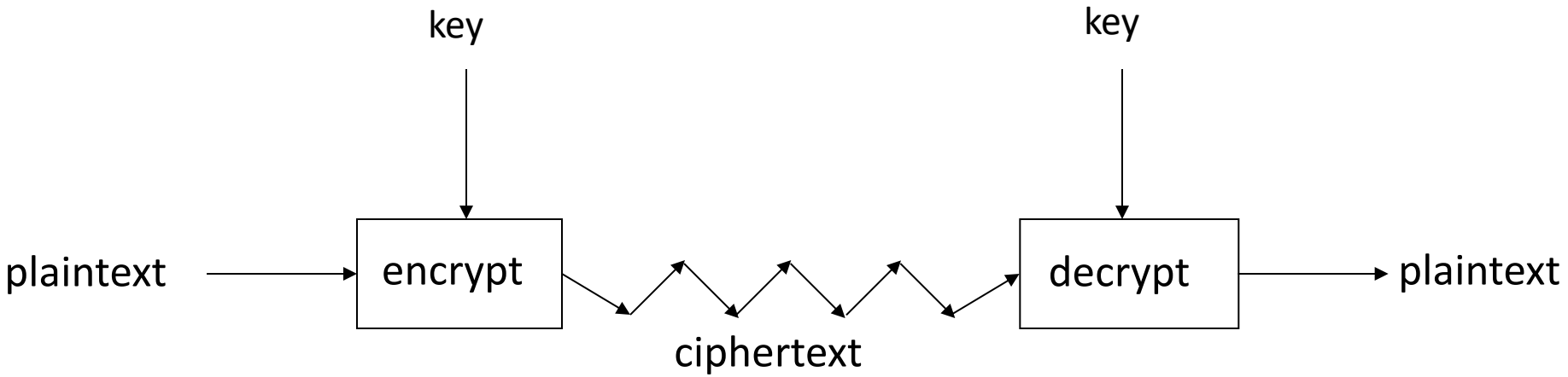
Cryptography Basics

- Classic Cryptography
  - Basics
  - Shift Ciphers (Caesar)
  - Vigenere and General Substitution cipher
  - (Double) transposition

Basics

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover the plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key (also called as "asymmetric key")* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

Crypto as Black Box



A generic view of symmetric key crypto

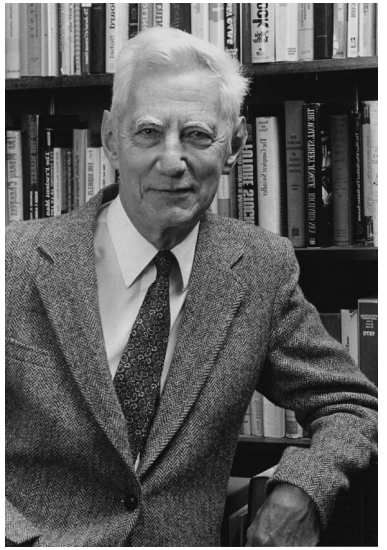
Principles

- Auguste Kerckhoffs (1835-1903)
  - The encryption algorithm must be **public**;

  the key remains **secret**.

- cf. *Journal des Sciences Militaires* Jan/Feb 1883).
- cf. *https://.../papers/kerckhoffs*.

Principles (cont.)



- Claude Shannon (1916-2001)
- Fundamental principles (properties for a “good” cryptosystem):
  - *confusion* (relation *plaintext – key/ciphertext* is obscure)
  - *diffusion* (spread plaintext through the ciphertext)

- Definition of secure (“information theoretic secure”):

"Perfect Secrecy" is defined by requiring of a system that after a cryptogram
is intercepted by the enemy the *a posteriori* probabilities of this cryptogram representing various messages be identically the same as the *a priori* probabilities of the same messages before the interception.

- In practice this means: there's *no short-cut* for exhaustive search.

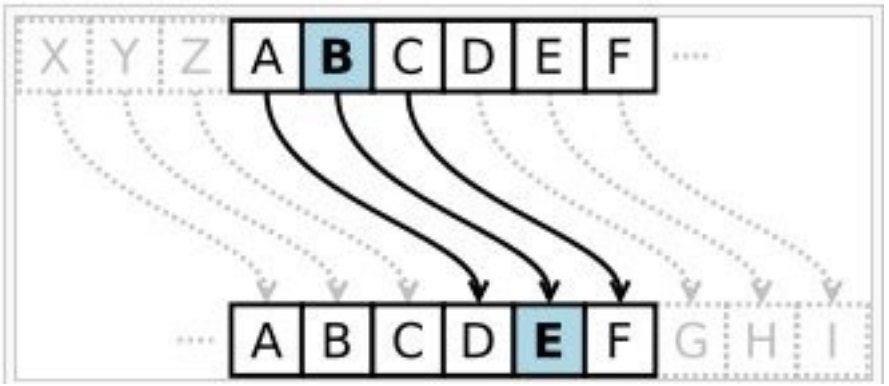
Principles (cont.)

- Substitution uses confusion: Change/replace letters
  - Characters (‘a’ → 'p’)
  - Words (cf. the Zimmerman telegram (1917))

- Transposition uses diffusion: Rearrange the letters
  - Less strong/effective than substitution

Shift Ciphers

- Simple versions are mono-alphabetic (fixed mapping of letters)
- One of the simplest is *Caesar* cipher: substitution (of each letter) using a 3-shift



- Generalization:

To *encrypt:*
$E_n(x) = (x + n) \% 26$

To *decrypt:*
$D_n(x) = (x - n) \% 26$

Caesar Example

- Plaintext: informationsecuritycourse
- Key:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

❗ What is the ciphertext?
(2 minutes)

Cryptanalysis: Shift Cipher

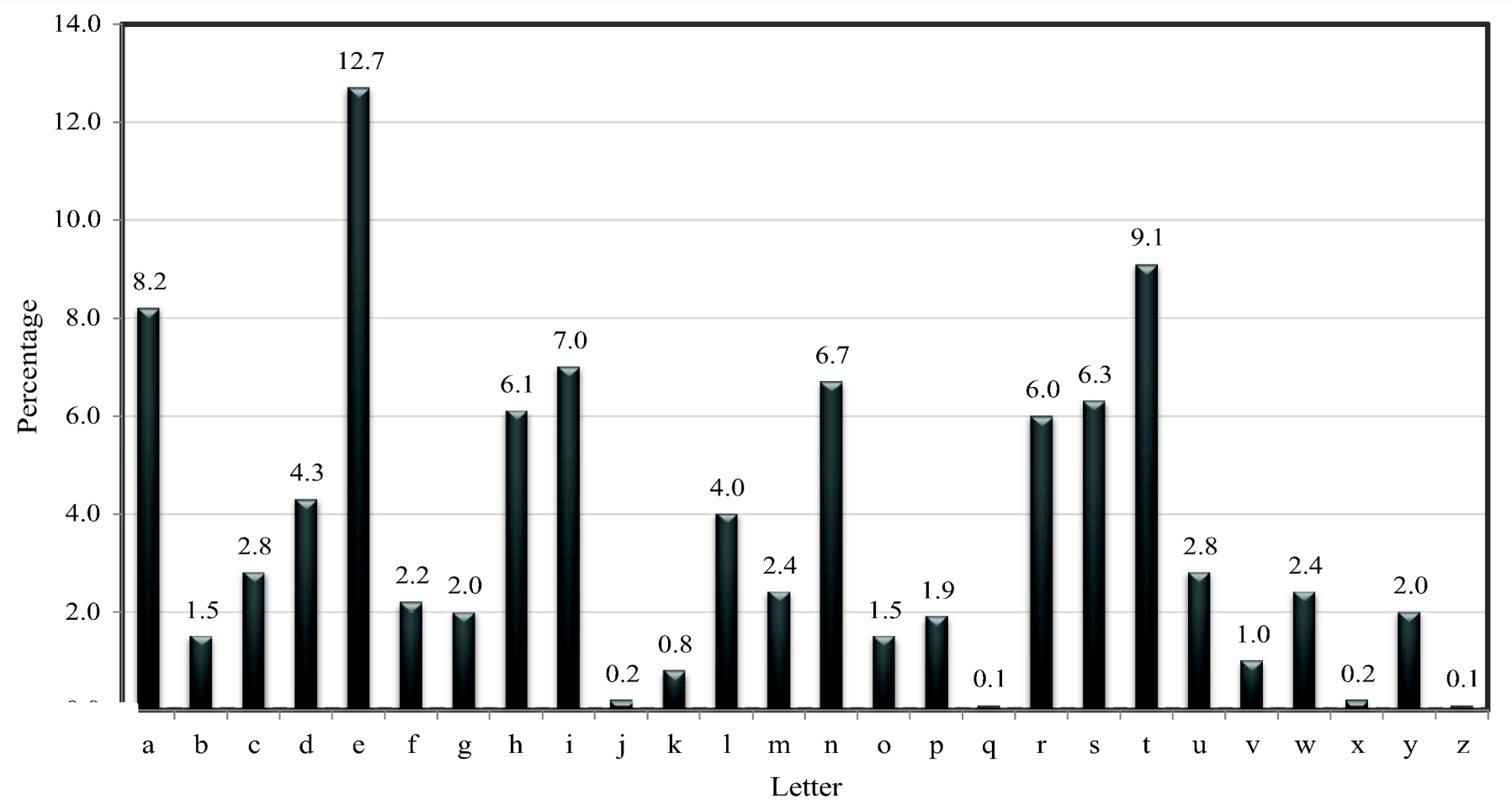
Is the Shift Cipher secure?

- No! Because there are 26 possible keys!
- A simple attack follows as (see the book or Katz's book for more details):
  - Given a ciphertext, try decrypting with every possible key
  - Only one possibility will "make sense" in the chosen language

- Example of a "brute-force" or "exhaustive-search" attack

```
lipps asvph
- khoor zruog
- jgnnq yqtnf
- ifmmp xpsme
- ?
```

Cryptanalysis:Using (plaintext) letter frequencies



Vigenere Cipher

- Poly-alphabetic Shift Cipher: no fixed shift value as in Caesar (e.g., 3) but varying values of shifts according to (key) letter positions
- The position (in the alphabet) of each key character represents the shift value, e.g. a =0, b=1, c=2 …
- Example, key = “cafe”, plaintext = “tellhimaboutme”

```
M: tellhimaboutme
K: cafecafecafeca
C: veqpjiredozxoe
```

Attacking the Vigenère cipher

- Key length is crucial! (Assume a 14-character key for the example)
- **Observation**: every 14th character is "encrypted" using the same shift

veqpjiredozxoe**u**alpcmsdjqu
iqn**d**nossoscdcusoa**k**jqmxpqr
hyycjq**o**qqodhjcciowie**i**i

- Looking at every 14th character

is (almost) like looking at ciphertext encrypted with the shift cipher

- Though a direct brute-force attack doesn't work…
- Why not?

Borrowed from the slides of Jonathan Katz [1]

Generalizing Shift Ciphers: **Substitution Ciphers**

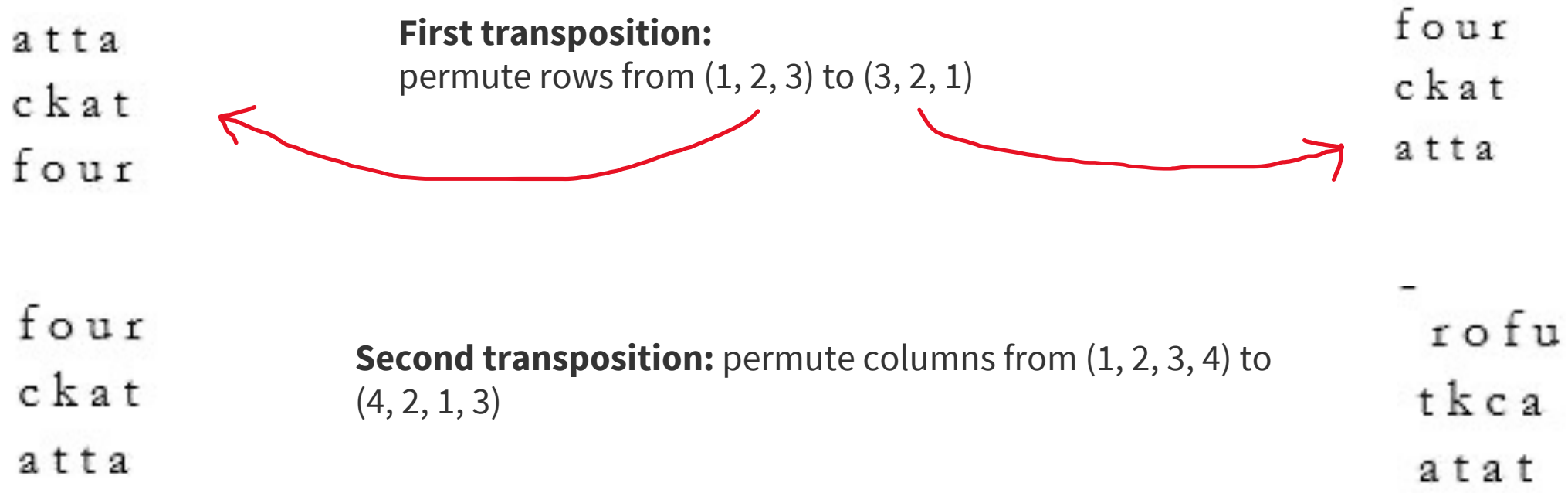
- Generalizing Caesar's substitution cipher:
  - Do not use a fixed shift, but a permutation: plaintext letters are mapped to a ciphertext letter (mapping is the key!)
  - 26 letters allow for *26! (approx. 2^{88}) possibilities*
  - Enormous Keyspace.

M:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C:	Z	P	B	Y	J	R	G	K	F	L	X	Q	N	W	V	D	H	M	S	U	T	O	I	A	Z	C

Anything wrong here?

Double Transposition

Assume the plain text: “attackatfour” and array size: 4



Transposition uses the principle “”?

More on Cryptanalysis

Systematic Analysis of cryptosystems in order to decipher the messages

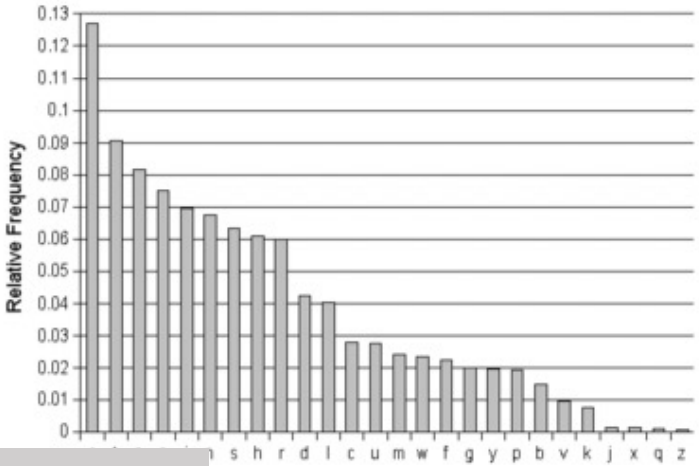
- **Ciphertext-only attack**: Trudy (the enemy) has access to the ciphertext c, and tries to recover the secret key k and the plaintext.

- **Known-plaintext attack**: Trudy knows the plaintext and the ciphertext. She tries to recover the secret key k. This is not uncommon at all!

- **Chosen-plaintext attack**: Trudy knows the plaintext but she is able to choose it herself. She gets the corresponding ciphertext. Her target is to recover the secret key k.
- …

More on Cryptanalysis (cont.)

- Language letter frequency tables:
  - Dutch: http://www.cryptogram.org/cdb/words/frequency.html
  - Other: http://codepad.clanhosts.com/index.php
    http://en.wikipedia.org/wiki/Letter_frequencies
- Techniques: anagramming, dictionary attacks…



- Large Keyspace: Sufficient key-space principle (SKSP)

Any secure encryption scheme must have a key space that is sufficiently large to make an exhaustive-search attack infeasible…

❗ Is SKSP a sufficient or a necessary condition for a secure cryptosystem?

What did we learn?

- Introduction to Information Security: *Perspectives*, *Objectives*, *Risks*
- Basic Encryption Techniques
  - Principles
  - Ceasar's Cipher,
  - Vigenere Cipher
  - (Generalized) Substitution Cipher
  - (Double) Transposition Cipher
- Cryptanalysis

References & Further Material

1. The slides of Katz & Lindell book:
   http://www.cs.umd.edu/~jkatz/crypto/s19/lectures.html

2. Web tool for classic cyphers:

https://www.dcode.fr/shift-cipher

Enough for today…

Questions