CS326 – Systems Security

Lecture 2

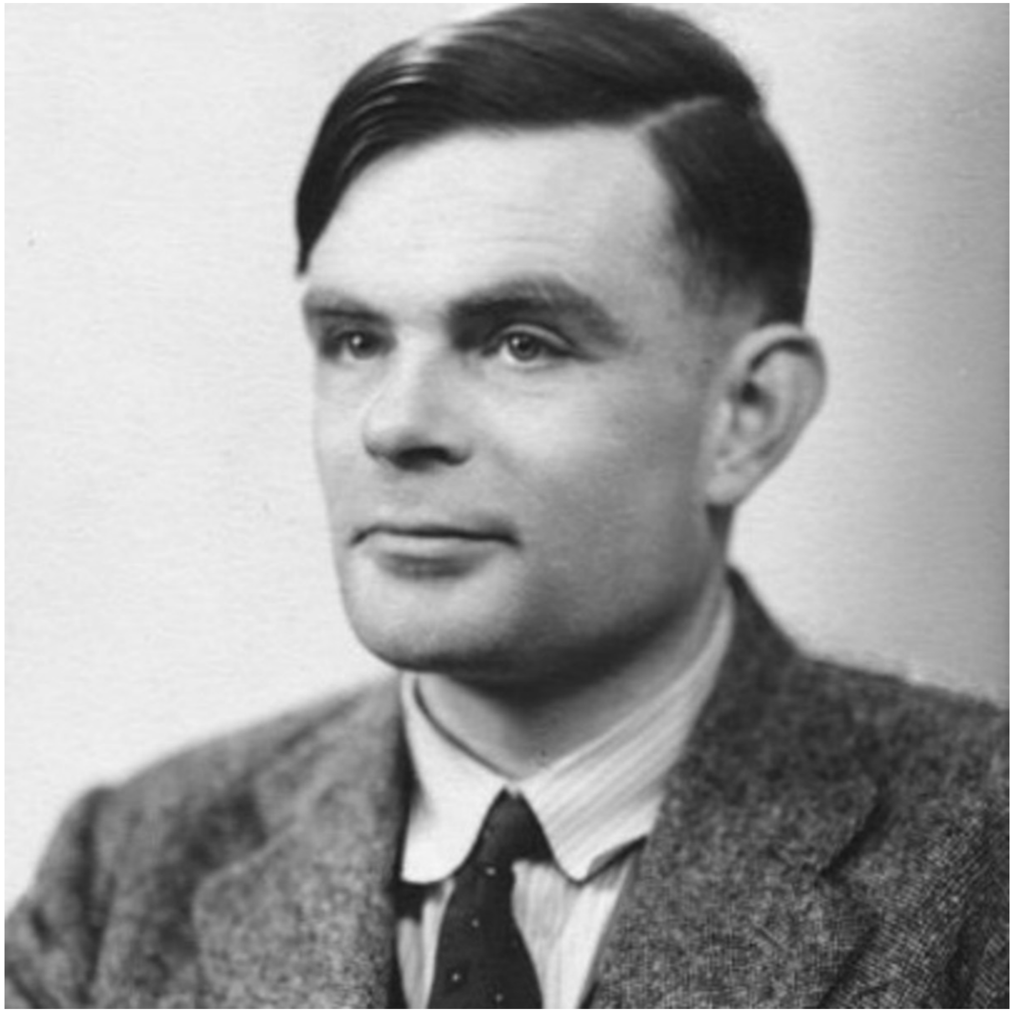
Introduction – Simple Ciphers

Elias Athanasopoulos
athanasopoulos.elias@ucy.ac.cy

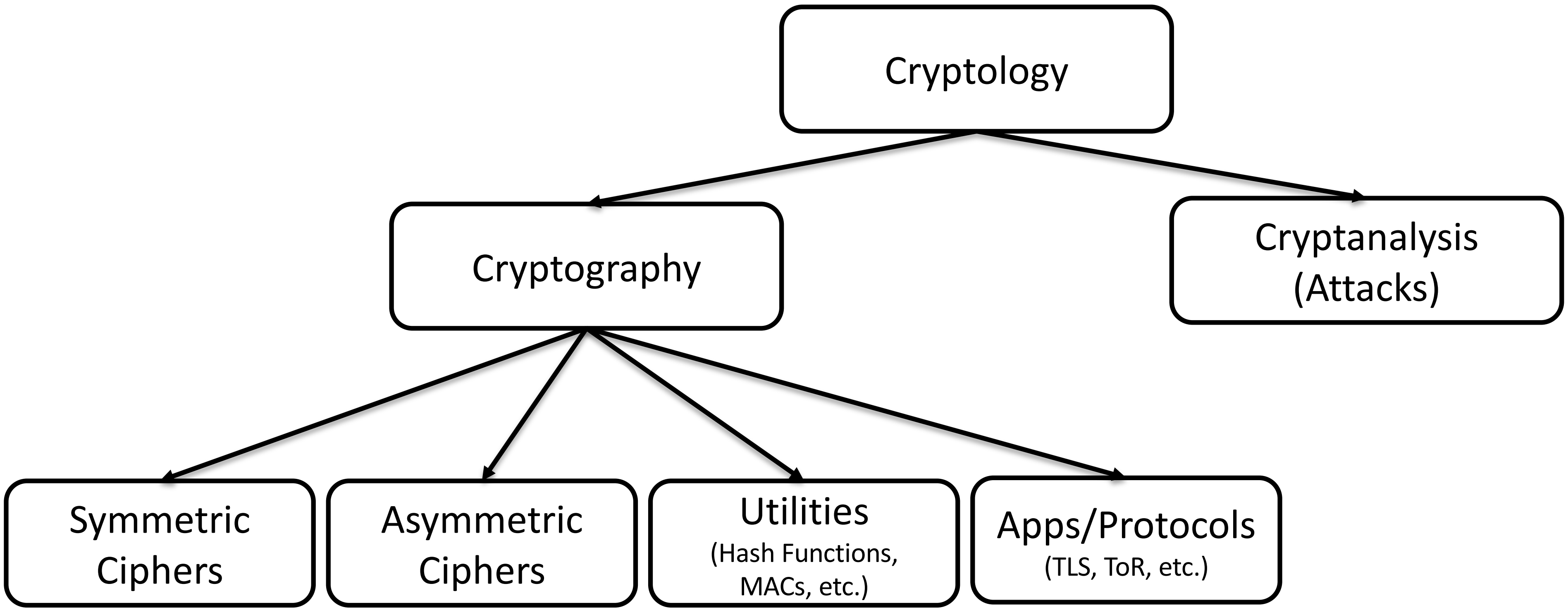
Sections of this lecture

- Introduction to Cryptography
- Simple Ciphers

INTRODUCTION TO CRYPTOGRAPHY



Cryptography Roadmap

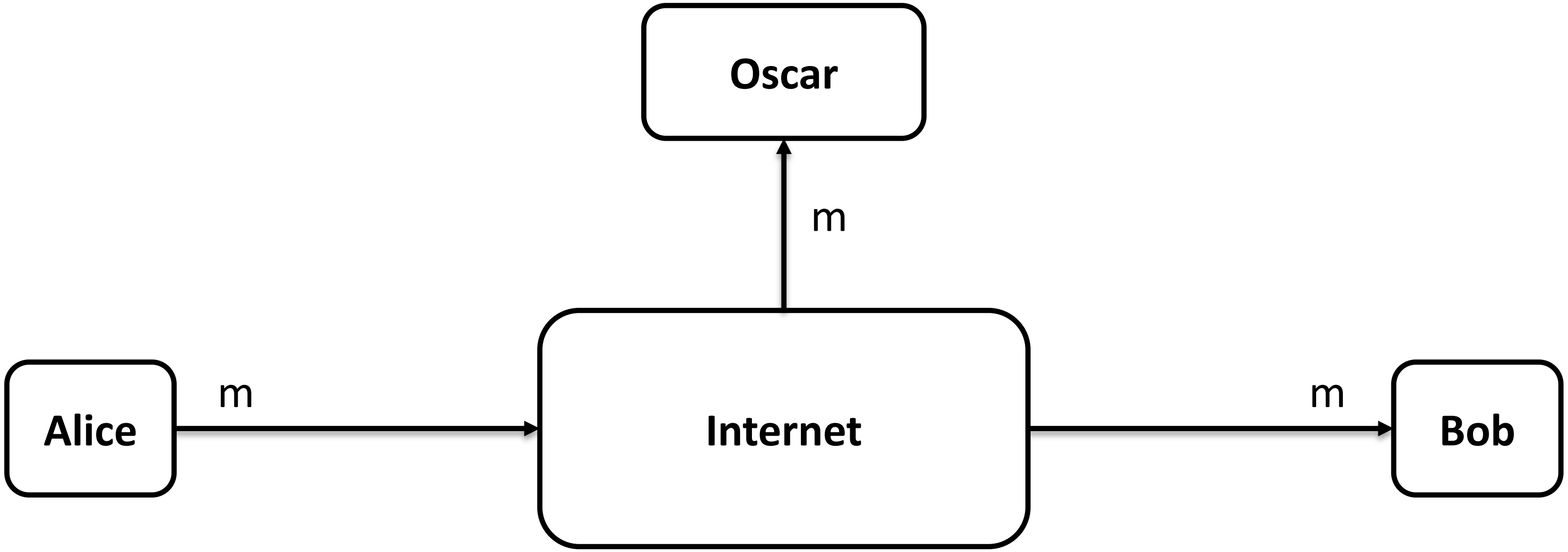


The Need for Cryptography

- People had always secrets
- Ordinary applications are based on secrecy
  - e.g., elections (or e-voting)
- Machines need to verify information
  - detect errors
- Unforgeable information
  - ordinary signatures vs digital signatures
- Many new applications
  - From car keys to smartcards, and cellphones

Basic Problem

Basic Problem

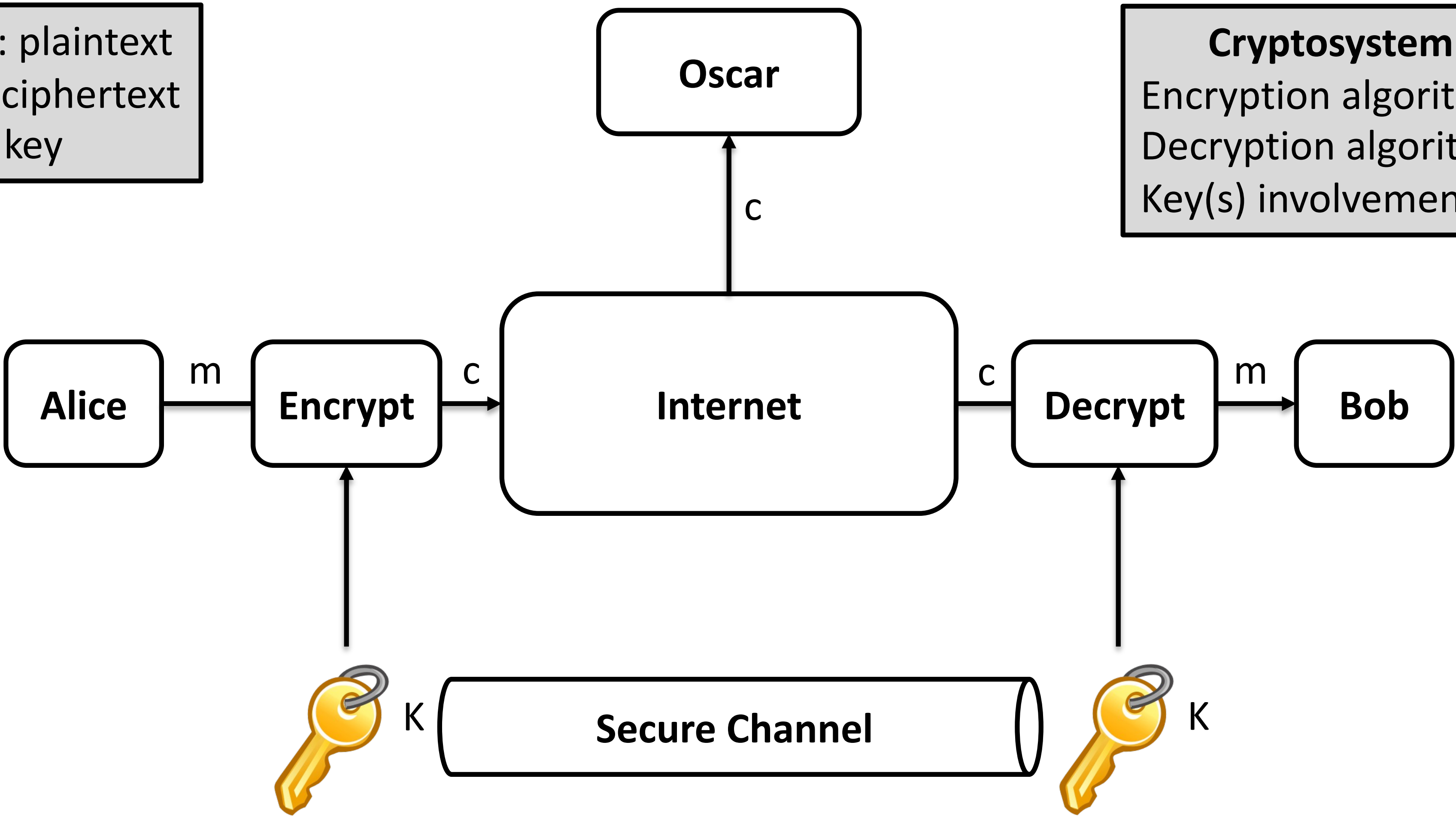


Oscar can see the message (confidentiality)
Oscar can modify the message (integrity)

Cryptographic Approach

m: plaintext
c: ciphertext
k: key

Cryptosystem
Encryption algorithm
Decryption algorithm
Key(s) involvement



Kerchoff’s Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge

~~Security via Obscurity~~

- All crypto algorithms are assumed to be **known**
- Security is based on
  - Secrecy of the key
  - Hard to infer the plaintext via the ciphertext
- Cryptanalysis
  - Infer the plaintext from ciphertext **without** knowing the key

SIMPLE CIPHERS

Simple Substitution Cipher

- Assume an alphabet
  - `abcdefghijklmnopqrstuvwxyz`
- Index the letters
  - *a* is 1, *b* is 2, *c* is 3, …, *z* is 26
- Select a key (secret), which **shifts** the order
  - Assuming the key is 3, then *a* is **shifted** three letters and becomes *d*, and *z* becomes *c* (wraps around the alphabet)

Caesar Cipher

a simple message ⇒ **$X \rightarrow X + key$**
(i.e., ‘a’ becomes ‘d’) ⇒ **dcwlpsohcp hwwdjh**

Encryption

$C = P + K \bmod 26$

Decryption

$P = C - K \bmod 26$

assuming an alphabet of 26 letters

Security Analysis

- Brute force attack
  - Key space is too small, 26 options
  - You need to just try 25 different keys
- All ciphers are vulnerable to brute force attack
  - If key space is too large, then attack is not practical
  - The cipher is then *Computationally Secure*

Multiple and Running Keys

- Vigenère Cipher

```
Key = r, u, n (three Caesar's keys)

tobeornottobethatisthequestion
runrunrunrunrunrunrunrunrunrun
KIOVIEEIGKIOVNURNVJNUVKHVMGZIA
```

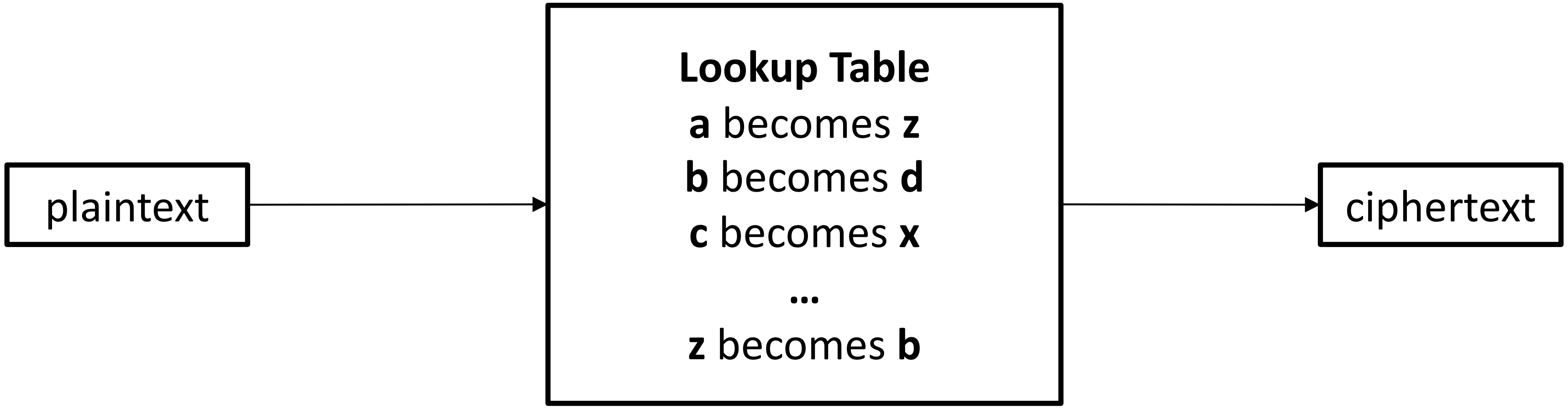
Secure Enough?

- Vigenère Cipher
  - **Problem 1**: repeated patterns in ciphertext

```
Key = r, u, n (three Caesar's keys)

tobeornottobethatisthequestion
runrunrunrunrunrunrunrunrunrun
KIOVIEEIGKIOVNURNVJNUVKHVMGZIA
```

Ideal Substitution Cipher



Key space: 26x25x24x..x1 = 26! ≈ 2^{88}

Frequency Analysis

- Simple substitution leaves the statistics of the plain message in the ciphertext
- A message of a known origin (e.g., English text) has no uniform letter distribution
- Letters **e**, **t**, and **a**, are more popular than **x**, **z**, and **v**

Letter Distribution in English Text

More Popular
Less popular

a	8.167%	n	6.749%
b	1.492%	o	7.507%
c	2.782%	p	1.929%
d	4.253%	q	0.095%
e	12.702%	r	5.987%
f	2.228%	s	6.327%
g	2.015%	t	9.056%
h	6.094%	u	2.758%
i	6.966%	v	0.978%
j	0.153%	w	2.360%
k	0.772%	x	0.150%
l	4.025%	y	1.974%
m	2.406%	z	0.074%

Example

Cipher

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

- q := E, h := A, r := T

  iq ifcc v**EE**r fb **T**d**E** vfllc**E** na Td**E** cfjw**A**wz **AT** bnnb **A**cc **A**ww**A**bs**E**v**E**b**T**e **A**w**E** v**A**l**E**

- After more iterations/trials

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

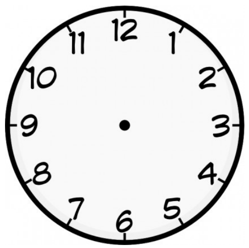
Modular Arithmetic

- In cryptography we use integers to express messages and then perform actions on them
  - For instance, Caesar cipher *shifts* each letter in the alphabet
- Modern ciphers are more complicated but they also work on finite sets of integers
  - Example one byte can take an integer value between 0 and 255

Modular Arithmetic

- Map the product of any computation (addition, multiplication) to a bounded set of integers
  - The bound is defined by the **modulus** (or base)
- Consider the analog clock, you can add several hours to a particular time, but the result will be always below 12h

  4h + 10h = 2h



Modular Arithmetic

Let a, r, m integers and $m > 0$, then

$a \equiv r \bmod m$, if m divides $a-r$

- Examples

$44 \equiv 2 \bmod 7$

$-9 \equiv 3 \bmod 6$

$11 \equiv 1 \bmod 5$

$18 \equiv 8 \bmod 10$

Equivalent Numbers

- Consider the set of integers for modulus 7
  - {0, 1, 2, 3, 4, 5, 6}
- All integers with reminder 1 form one set
  - {…, -13, -6, 1, 8, 15, 22, … }
- All integers with reminder 2 form one set
  - {…, -12, -5, 2, 9, 16, 23, … }
- For each set, all numbers are equivalent in modulus 7 arithmetic
- **Example**: 529 mod 7?

  529 = 23*23 mod 7 = 2*2 mod 7 = 4 mod 7

Transposition Cipher

- Instead of substituting letters, re-arrange them

t	h	i	s		i	s	
a		f	u	n	k	y	
m	e	s	s	a	g	e	
p	e	r	m	u	t	e	d

↓

t	a	m	p	h		e	e
i	f	s	r	s	u	s	m
	n	a	u	i	k	g	t
s	y	e	e				d

Scytale

Resources

- This lecture was built using material that can be found at
  - Chapter 7, Handbook of Applied Cryptography, http://cacr.uwaterloo.ca/hac/
  - Chapter 1, Understanding Cryptography, http://www.crypto-textbook.com