COMPSCI 4CR3 - Applied Cryptography

Jake Doliskani

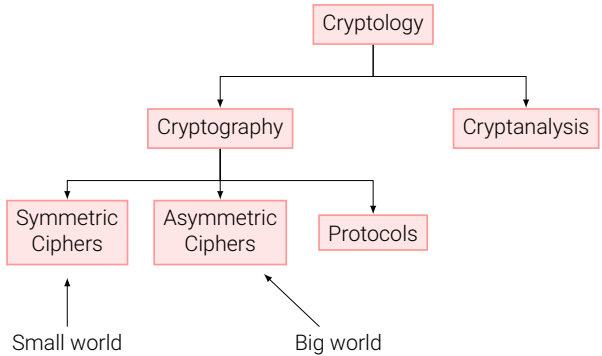
McMaster University

Introduction to Cryptography

This lecture

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

Overview


Cryptology
Cryptography
Cryptanalysis
Symmetric Ciphers
Asymmetric Ciphers
Protocols
Small world
Big world

Cryptography

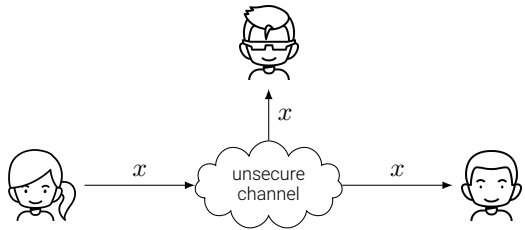
is the science/art of protecting secrets.

Pre-modern cryptography

- Very old
  Scytale of Sparta, Caesar cipher

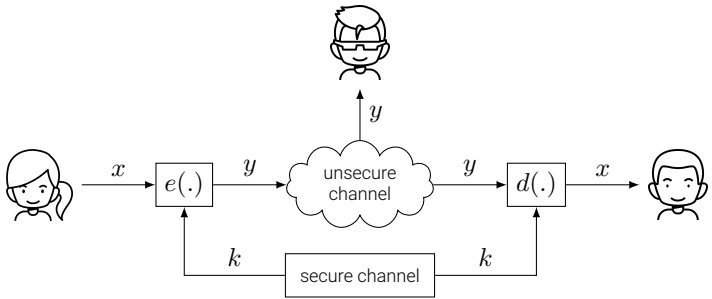
- More recent
  Enigma

Symmetric Cryptography



- Alice and Bob want to communicate over an unsecure channel
- Trudy has access to the channel but should not be able to understand the messages

Symmetric Cryptography



- x is the plaintext
- y is the ciphertext
- k is the key

Symmetric Cryptography

- The encryption $y = e_k(x)$ and decryption $x = d_k(y)$ must be inverse to each other:
$$d_k(e_k(x)) = x \text{ for all messages } x.$$
- The encryption and decryption algorithms are public; everyone knows them.
- The system is only secure if the key is shared between Alice and Bob in a secure way
  - This can be done by public key cryptography (later in the course)

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

The Substitution Cipher

- Substitute symbols using a permutation.
- The permutation is the key
- Alphabet example:

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	,	‘	;	.	?
y	e	q	j	u	l	’	w	s	r	p	i	f	x	t	h	m	.	z	k	,	d	;	v	o	a	b	g	?	c	n

`information` ⟹ `sxt.fykstx`

The Substitution Cipher

Attacks

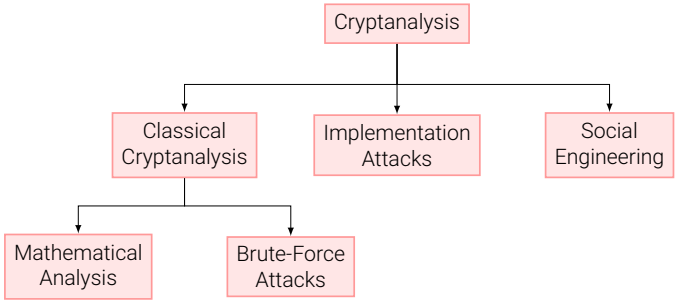
- Brute-Force
  - Try all possible keys
  - Slow; for example, for 31 symbols, there are $\approx 2^{112}$ keys.
- Letter Frequency Analysis
  - Determine the frequency of every ciphertext letter
  - Compare with the frequency distribution of the language

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

```
We will meet in the middle of the library at noon
all arrangements are made
```

e	0.12702	m	0.02406
t	0.09056	w	0.0236
a	0.08167	f	0.02228
o	0.07507	g	0.02015
i	0.06966	y	0.01974
n	0.06749	p	0.01929
s	0.06327	b	0.01492
h	0.06094	v	0.00978
r	0.05987	k	0.00772
d	0.04253	j	0.00153
l	0.04025	x	0.0015
c	0.02782	q	0.00095
u	0.02758	z	0.00074

Cryptanalysis



- **Implementation attacks:** try to extract the key using side channel techniques, e.g. power analysis.
- **Social engineering:** try to obtain the information about the key using social interactions.

Why do we need cryptanalysis?

- There is no (and probably will never be) mathematical proof of security for any practical cipher
- The only way to have assurance that a cipher is secure is to try to break it (and fail)!

Only use cryptosystems that are well established, i.e., have been cryptanayzed for many years.

Kerckhoffs' Principle

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

How Many Key Bits Are Enough?

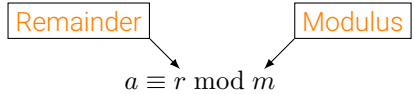
- Key length is estimated based on the best known attack
- Key lengths for symmetric and asymmetric algorithms are dramatically different

Example: for successful brute-force attacks on symmetric algorithms:

Key length	Security estimation
56–64 bits	short term: a few hours or days
112–128 bits	long term: several decades in the absence of quantum computers
256 bits	long term: several decades, maybe even with quantum computers

Modular Arithmetic

Modulo operation:



- It means $m \mid a - r$ (m divides $a - r$)
- Equivalently, $a = mq + r$ for some integer q.

Example: $73 \equiv 8 \bmod 13$.

- The remainder r is not unique: $73 \equiv 21, -15 \bmod 13$
- There is an infinite set of such remainders: $\{\dots, -18, -5, 8, 21, \dots\}$
- This is called an equivalence class. We can use any of the members in this equivalence class in operations modulo 13.

We usually choose r such that $0 \leq r < m$.

Modular Arithmetic

- We compute modular division by multiplying by the inverse, i.e. $a/b \bmod m$ is $ab^{-1} \bmod m$.
  - The inverse b^{-1} of b satisfies $bb^{-1} \equiv 1 \bmod m$.
  - Example: to compute $3/5 \bmod 9$, we first find $5^{-1} \equiv 2 \bmod 9$ and then compute $3 \cdot 2 \equiv 6 \bmod 9$.

- The inverse b^{-1} exists only if $\gcd(b, m) = 1$.
  - In this case, we say b and m are coprime.
  - We sometimes write $(b, m) = 1$ instead

Modular Arithmetic

- Modular reduction can be performed at any point of computation
- Example: exponentiation
  - Modular reduction at the end:

$$7^5 = 16807 \equiv 11 \bmod 13$$

  - Modular reduction throughout:

$$7^5 = 7^2 \cdot 7^2 \cdot 7 \equiv 10 \cdot 10 \cdot 7 \equiv 11 \bmod 13$$

It is usually computationally cheaper to perform intermediate modular reduction.

Modular Arithmetic (Integer Rings)

The integer ring is the set $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ on which we define two operations:

- Multiplication: $a \times b$ is defined as $a \times b \bmod m$ for all $a, b \in \mathbb{Z}_m$.
- Addition: $a + b$ is defined as $a + b \bmod m$ for all $a, b \in \mathbb{Z}_m$.

Example: $\mathbb{Z}_7 = \{0, 1, \ldots, 7\}$ with addition and multiplication $\bmod 7$.

Integer rings are special cases of general rings.

Modular Arithmetic (Integer Rings)

A ring R is a set with the following properties for all $a, b, c \in R$:

- Closure: The results of addition and multiplication are always in R.
- Associativity:

$$a + (b + c) = (a + b) + c$$
$$a \times (b \times c) = (a \times b) \times c$$

- Distributive law: $a \times (b + c) = (a \times b) + (a \times c)$
- Neutral element for addition: $a + 0 = a$
- Neutral element for multiplication: $a \times 1 = a$
- Additive inverse: $a + (-a) = 0$
- Multiplicative inverse: $a \times a^{-1} = 1$ (might not always exists)

The Caesar Cipher

Shift each symbol (and wrap around)

- Key: $k \in \mathbb{Z}_m$
- Plaintext: $x \in \mathbb{Z}_m$
- Ciphertext: $y \in \mathbb{Z}_m$

Encryption: $e_k(x) \equiv x + k \bmod m$
Decryption: $d_k(y) \equiv y - k \bmod m$

Example: the alphabet

- $m = 26$
- Key: $k = 17$

Palintext: `attack` $= 0, 19, 19, 0, 2, 10$.
Ciphertext: $17, 10, 10, 17, 19, 1 =$ `rkkrtb`

The Affine Cipher

Transform each symbol by a linear map

- Key: $a, b \in \mathbb{Z}_m$, where a is invertible $\bmod m$
- Plaintext: $x \in \mathbb{Z}_m$
- Ciphertext: $y \in \mathbb{Z}_m$

Encryption: $e_k(x) \equiv ax + b \bmod m$
Decryption: $d_k(y) \equiv a^{-1}(y - b) \bmod m$

Example: the alphabet

- $m = 26$
- Key: $(a, b) = (9, 13)$, where $a^{-1} \equiv 3 \bmod 26$

Palintext: $\texttt{attack} = 0, 19, 19, 0, 2, 10$.
Ciphertext: $13, 2, 2, 13, 5, 25 = \texttt{nccnfz}$