EDIN01: Cryptography - Reference Sheet

Karl Hallsby

Last Edited: November 5, 2019

Contents

1 Cryptography Introduction

Defn 1 (Cryptographic Primitive)**.** A *cryptographic primitive* is an algorithm with basic cryptographic properties.

Defn 2 (Cryptographic Protocol)**.** A *cryptographic protocol* involves the back-and-forth communication among two or more parties.

Remark 2.1 (Bob and Alice). Typically, the parties are named Bob and Alice. These are arbitrary names, but these are the most commonly used ones.

There are have been several Cryptographic Protocols.

1. *Symmetric-key cryptography* - Methods in which both the sender and receiver share the same key
    (a) Block ciphers
    (b) Stream ciphers
    (c) MAC algorithms
2. *Public-key cryptography*: 2 different, but mathematically related keys are used. A public key and a private key.
    (a) The public key cannot decrypt something that was encrypted with the private key.
    (b) The public key can be shared freely, because the private key cannot be generated from the public key.
3. *Cryptographic hash functions* are a related and important class of cryptographic algorithms.
    (a) This is a keyless Cryptographic Primitive.
    (b) Takes an arbitrary length input and produces a fixed-length output.
    (c) The mapping between the input and output is such that the output cannot generate the input, therefore making it cryptographic.

1.1 Historical Cryptography

Just to give a super quick background on how we've gotten to where we are today when it comes to cryptography.

1.1.1 Monoalphabetic Ciphers

Defn 3 (Monoalphabetic Cipher)**.** In a *monoalphabetic cipher* a single letter is replaced by the cipher's mapping. Since the cipher can do this to arbitrary letters, this could continue indefinitely for any single letter.

These were some of the first ciphers developed by Man. These include simple substitute ciphers, and letter shifting ciphers. However, these can be broken with *frequency analysis*.

1.1.2 Polyalphabetic Ciphers

Defn 4 (Polyalphabetic Cipher)**.** In a *polyalphabetic cipher* multiple letters are replaced by the cipher's mapping. Additionally, since the cipher can output multiple letters, the ciphered letters could be run through the cipher again.

These were developed in response to Monoalphabetic Ciphers being broken. However, these can also be broken, with *extended frequency analysis*.

Eventually, it was realized that the secrecy of the cipher is not sensible/possible. This leads us to the conclusion that **any cryptographic scheme should remain secure even if the adversary understands the cipher algorithm itself**.

1.1.3 Cryptographic Keys

The use of keys as ciphers is a slightly more modern occurrence.

Defn 5 (Kerckhoff's Principle)**.** *Kerckhoff's Principle* states that the security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. Essentially, the security of the key used should be sufficient such that the cipher can be maintained confidently while under attack.

However, only since the mid-1970s, has public key cryptography has been possible.
Computers can efficiently encrypt, given the following constraints:

1. Some modern techniques can only keep the keys secret if certain mathematical problems are Intractable.
    (a) Integer factorization
    (b) Discrete logarithm problems
2. However, there are no absolute proofs that a cryptographic technique is secure.

Defn 6 (Intractable)**.** An *intractable* problem is one in which there are no **efficient** algorithms to solve them.

Symmetric-Key Cryptography	Public-Key Cryptography
Block ciphers	Public-Key encryption
Stream ciphers	Digital Signature Schemes
Cryptographic Hash Functions	Key exchange protocols
	Electronic Cash/Cryptocurrency
	Interactive Proof Systems

Table 1.1: Uses of Key-Based Cryptography

2 Number Theory

Before we can start with any of the deeper cryptography stuff, we need to start with some basic number theory.

Defn 7 (Number Theory)**.** *Number theory* is a branch of pure mathematics devoted primarily to the study of the integers and integer-valued functions. Number theorists study prime numbers as well as the properties of objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers).

Defn 8 (Divides)**.** For $a, b \in \mathbb{Z}$, we say that a *divides* b (written $a \mid b$) if there exists an integer c such that $b = ac$.

Properties:

(i) $a \mid a$

(ii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

(iv) If $a \mid b$ and $b \mid a$, then $a = \pm b$.

2.1 Quotient and Remainder

For $a, b \in \mathbb{Z}$, with $b \geq 1$. Then an ordinary long division of a by b, i.e. $a \div b$ yields two integers q and r such that

$$a = qb + r, \text{where } 0 \leq r < b \tag{2.1}$$

q and r are called the Quotient and Remainder, respectively, and are **unique**.

Defn 9 (Quotient)**.** The *quotient*, q, of a divided by b is denoted $a \operatorname{div} b$.

Defn 10 (Remainder)**.** The *remainder*, r, of a divided by b is denoted $a \bmod b$.

Example 2.1: Quotient and Remainder.

If $a = 53$ and $b = 9$, what is $a \bmod b$?

$$\begin{aligned} 53 &= q9 + r \\ q &= 5 \\ r &= 8 \end{aligned}$$

2.2 Greatest Common Divisor

Defn 11 (Common Divisor)**.** An integer c is a *common divisor* of a and b if $c \mid a$ and $c \mid b$.

Defn 12 (Greatest Common Divisor)**.** A non-negative integer d is called the *greatest common divisor* (*GCD*) of integers a and b if:

1. d is a Common Divisor of a and b.
2. For every other common divisor c it holds that $c \mid d$.

The greatest common divisor is denoted

$$\gcd(a, b) \tag{2.2}$$

$\gcd(a, b)$ is the **largest positive** integer dividing both a and b (except for $\gcd(0, 0) = 0$).

Remark 12.1. If $a, b \in \mathbb{Z}^+$, then $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

Example 2.2: Greatest Common Divisor.

What is the $\gcd(18, 24)$?

Common Divisors = $\{\pm 1, \pm 2, \pm 4, \pm 6\}$.
Since we can only allow positive integers,

$$\gcd(18, 24) = +6$$

2.3 Least Common Multiple

Defn 13 (Least Common Multiple)**.** A non-negative integer d is called the *least common multiple* (LCM) of integers a and b if:

1. $a \mid d$ and $b \mid d$
2. For every integer c such that $a \mid c$ and $b \mid c$, we have $d \mid c$.

The least common multiple is denoted

$$\operatorname{lcm}(a, b) \tag{2.3}$$

$\operatorname{lcm}(a, b)$ is the **smallest positive** integer divisible by both a and b.

Remark 13.1. If $a, b \in \mathbb{Z}^+$, then $\operatorname{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$

2.4 Primality

Defn 14 (Relatively Prime)**.** a, b are called *relatively prime* if $\gcd(a, b) = 1$.

Defn 15 (Prime)**.** An integer $p \geq 2$ is called *prime* if its only positive divisors are 1 and p. Otherwise, p is called a *Composite.*

Defn 16 (Composite)**.** An integer $p \geq 2$ is called *composite* if it has more positive divisors than just 1 and p. Otherwise, p is called a *Prime.*

2.4.1 Number of Primes

The number of primes $\leq x$ is denoted

$$\pi(x) \tag{2.4}$$

1. There are infinitely many primes
2. $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$
3. For $x \geq 17$, $\frac{x}{\ln(x)} < \pi(x) < \frac{1.25506x}{\ln(x)}$

2.5 Unique Factorization

Theorem 2.1 (Unique Factorization Theorem)**.** *Every integer $n \geq 2$ can be written as a product of prime powers,*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \ldots p_k$ are distinct primes and $e_1, e_2, \ldots e_k$ are positive integers. Furthermore, the factorization is unique up to rearrangement of the factors.

2.5.1 Greatest Common Divisor and Least Common Multiple with Unique Factors

If $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{e_k}$, where $e_i, f_i, i = 1, 2, \ldots k$ are non-negative integers, then

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)} \tag{2.5}$$

and

$$\operatorname{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)} \tag{2.6}$$

2.6 Euler Phi Function

Defn 17 (Euler Phi Function)**.** For $n \geq 1$, let $\phi(n)$ denote the number of integers in the interval $[1, n]$, which are Relatively Prime to n. This function is called the *Euler Phi Function.*

Theorem 2.2 (Euler Phi Function)**.** *There are a few properties of the Euler Phi Function that we will treat as true because of this theorem.*

1. *If p is a Prime, then $\phi(p) = p - 1$.*
2. *If $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$.*
3. *If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then*

$$\phi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right) \cdots \left(p_k^{e_k} - p_k^{e_k-1}\right)$$

Lemma 2.3 (Computing the Greatest Common Divisor)*.* If a and b are positive integers where $a > b$, then

$$\gcd(a, b) = \gcd(b, a \bmod b) \tag{2.7}$$

Remark. This can be repeated to efficiently calculate the $\gcd(a, b)$. This is called the Euclidean Algorithm.

Defn 18 (Euclidean Algorithm)**.** The *euclidean algorithm* is a way to efficiently calculate the $\gcd(a, b)$.

```
1. Set $r_0 \leftarrow a, r_1 \leftarrow b, i \leftarrow 1$.
2. While $r_i \neq 0$ do:
    (a) Set $r_{i+1} \leftarrow r_{i-1} \bmod r_i, i \leftarrow i + 1$
3. Return $r_i$
```

Example 2.3: Euclidean Algorithm.

Find the Greatest Common Divisor of 147 and 273?

$$\begin{aligned} 273 &= 1 \cdot 147 + 126 \Rightarrow \gcd(126, 147) \\ 147 &= 1 \cdot 126 + 21 \Rightarrow \gcd(21, 126) \\ 126 &= 6 \cdot 21 + 0 \Rightarrow \gcd(21, 126) \end{aligned}$$

Thus, since $6 \cdot 21 = 126$, 21 is the Greatest Common Divisor of 147 and 273.

Theorem 2.4. *There exist integers x, y such that $\gcd(a, b)$ can be written as*

$$\gcd(a, b) = ax + by \tag{2.8}$$

Proof.

$$\begin{aligned} \gcd(a, b) &= r_i \\ &= r_{i-2} - q_{i-1} r_{i-1} \\ &= r_{i-2} - q_{i-1}(r_{i-3} - q_{i-2} r_{i-2}) \\ &\vdots \\ &= r_0 x + r_1 y \\ &= ax + by \end{aligned}$$

for some integers $x, y \in \mathbb{Z}$. ■

This means that the Euclidean Algorithm can be extended to return the values of x and y from Equation (2.8).

2.7 The Integers modulo n

Let n be a positive integer. If a and b are integers, then *a is said to be congruent to b modulo n*, which is written as

$$a \equiv b \pmod{n} \tag{2.9}$$

If n divides $(a-b)$, i.e. $n\,|(a-b)$, then we call n the *modulus* of the congruence.

Theorem 2.5. *For $a, a_1, b, b_1, c \in \mathbb{Z}$, we have*

(i) $a \equiv b \pmod{n}$ if and only if *a and b leave the same Remainder when divided by n.*

(ii) $a \equiv a \pmod{n}$

(iii) *If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$*

(iv) *If $a \equiv b \pmod{n}$ adn $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$*

(v) *If $a \equiv a_1 \pmod{n}$ and $b \equiv b_1 \pmod{n}$, then $a+b = a_1+b_1 \pmod{n}$ and $ab = a_1b_1 \pmod{n}$.*

*The properties **(ii)** to **(iv)** are called* reflexivity*,* symmetry*, and* transitivity*, respectively.*

2.8 Equivalence Classes

Defn 19 (Equivalence Class)**.** Congruence modulo n partitions $\mathbb{Z}$ into n sets, called *equivalence class*es, where each integer belongs to exactly one equivalence class.

For example, these are all congruent to each other modulo n:

$$\{\ldots, -2n, -n, 0, n, 2n, \ldots\} \tag{2.10a}$$

$$\{\ldots -2n+1, -n+1, 1, n+1, 2n+1 \ldots\} \tag{2.10b}$$

Since all elements in an equivalent class have the same Remainder, r, we use r as a *represenatative* for the equivalence class.

Remark 19.1. In this case, the representatives of the equivalence classes shown in Equations (2.10a) to (2.10b) are 0 and 1, respectively.

A Complex Numbers

Complex numbers are numbers that have both a real part and an imaginary part.

$$z = a \pm bi \tag{A.1}$$

where

$$i = \sqrt{-1} \tag{A.2}$$

Remark (i vs. j for Imaginary Numbers). Complex numbers are generally denoted with either i or j. Since this is an appendix section, I will denote complex numbers with i, to make it more general. However, electrical engineering regularly makes use of j as the imaginary value. This is because alternating current i is already taken, so j is used as the imaginary value instad.

$$Ae^{-ix} = A\left[\cos(x) + i\sin(x)\right] \tag{A.3}$$

A.1 Complex Conjugates

If we have a complex number as shown below,

$$z = a \pm bi$$

then, the conjugate is denoted and calculated as shown below.

$$\overline{z} = a \mp bi \tag{A.4}$$

Defn A.1.1 (Complex Conjugate)**.** The conjugate of a complex number is called its *complex conjugate*. The complex conjugate of a complex number is the number with an equal real part and an imaginary part equal in magnitude but opposite in sign.

The complex conjugate can also be denoted with an asterisk ($*$). This is generally done for complex functions, rather than single variables.

$$z^* = \overline{z} \tag{A.5}$$

A.1.1 Complex Conjugates of Exponentials

$$\overline{e^z} = e^{\overline{z}} \tag{A.6}$$

$$\overline{\log(z)} = \log(\overline{z}) \tag{A.7}$$

A.1.2 Complex Conjugates of Sinusoids

Since sinusoids can be represented by complex exponentials, as shown in Appendix B.2, we could calculate their complex conjugate.

$$\begin{aligned}\overline{\cos(x)} &= \cos(x) \\ &= \frac{1}{2}\left(e^{ix} + e^{-ix}\right)\end{aligned} \tag{A.8}$$

$$\begin{aligned}\overline{\sin(x)} &= \sin(x) \\ &= \frac{1}{2i}\left(e^{ix} - e^{-ix}\right)\end{aligned} \tag{A.9}$$

B Trigonometry

B.1 Trigonometric Formulas

$$\sin(\alpha) + \sin(\beta) = 2\sin\left(\frac{\alpha+\beta}{2}\right)\cos\left(\frac{\alpha-\beta}{2}\right) \tag{B.1}$$

$$\cos(\theta)\sin(\theta) = \frac{1}{2}\sin(2\theta) \tag{B.2}$$

B.2 Euler Equivalents of Trigonometric Functions

$$e^{\pm j\alpha} = \cos(\alpha) \pm j\sin(\alpha) \tag{B.3}$$

$$\cos(x) = \frac{e^{jx} + e^{-jx}}{2} \tag{B.4}$$

$$\sin(x) = \frac{e^{jx} - e^{-jx}}{2j} \tag{B.5}$$

$$\sinh(x) = \frac{e^{x} - e^{-x}}{2} \tag{B.6}$$

$$\cosh(x) = \frac{e^{x} + e^{-x}}{2} \tag{B.7}$$

B.3 Angle Sum and Difference Identities

$$\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta) \tag{B.8}$$

$$\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) \tag{B.9}$$

B.4 Double-Angle Formulae

$$\sin(2\alpha) = 2\sin(\alpha)\cos(\alpha) \tag{B.10}$$

$$\cos(2\alpha) = \cos^2(\alpha) - \sin^2(\alpha) \tag{B.11}$$

B.5 Half-Angle Formulae

$$\sin\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1-\cos(\alpha)}{2}} \tag{B.12}$$

$$\cos\left(\frac{\alpha}{2}\right) = \sqrt{\frac{1+\cos(\alpha)}{2}} \tag{B.13}$$

B.6 Exponent Reduction Formulae

$$\sin^2(\alpha) = \frac{1-\cos(2\alpha)}{2} \tag{B.14}$$

$$\cos^2(\alpha) = \frac{1+\cos(2\alpha)}{2} \tag{B.15}$$

B.7 Product-to-Sum Identities

$$2\cos(\alpha)\cos(\beta) = \cos(\alpha-\beta) + \cos(\alpha+\beta) \tag{B.16}$$

$$2\sin(\alpha)\sin(\beta) = \cos(\alpha-\beta) - \cos(\alpha+\beta) \tag{B.17}$$

$$2\sin(\alpha)\cos(\beta) = \sin(\alpha+\beta) + \sin(\alpha-\beta) \tag{B.18}$$

$$2\cos(\alpha)\sin(\beta) = \sin(\alpha+\beta) - \sin(\alpha-\beta) \tag{B.19}$$

B.8 Sum-to-Product Identities

$$\sin\left(\alpha\right) \pm \sin\left(\beta\right) = 2\sin\left(\frac{\alpha \pm \beta}{2}\right)\cos\left(\frac{\alpha \mp \beta}{2}\right) \tag{B.20}$$

$$\cos\left(\alpha\right) + \cos\left(\beta\right) = 2\cos\left(\frac{\alpha + \beta}{2}\right)\cos\left(\frac{\alpha - \beta}{2}\right) \tag{B.21}$$

$$\cos\left(\alpha\right) - \cos\left(\beta\right) = -2\sin\left(\frac{\alpha + \beta}{2}\right)\sin\left(\frac{\alpha - \beta}{2}\right) \tag{B.22}$$

B.9 Pythagorean Theorem for Trig

$$\cos^2\left(\alpha\right) + \sin^2\left(\alpha\right) = 1^2 \tag{B.23}$$

B.10 Rectangular to Polar

$$a + jb = \sqrt{a^2 + b^2}e^{j\theta} = re^{j\theta} \tag{B.24}$$

$$\theta = \begin{cases} \arctan\left(\frac{b}{a}\right) & a > 0 \\ \pi - \arctan\left(\frac{b}{a}\right) & a < 0 \end{cases} \tag{B.25}$$

B.11 Polar to Rectangular

$$re^{j\theta} = r\cos\left(\theta\right) + jr\sin\left(\theta\right) \tag{B.26}$$

C Calculus

C.1 Fundamental Theorems of Calculus

Defn C.1.1 (First Fundamental Theorem of Calculus)**.** The *first fundamental theorem of calculus* states that, if f is continuous on the closed interval $[a, b]$ and F is the indefinite integral of f on $[a, b]$, then

$$\int_a^b f(x)\,dx = F(b) - F(a) \tag{C.1}$$

Defn C.1.2 (Second Fundamental Theorem of Calculus)**.** The *second fundamental theorem of calculus* holds for f a continuous function on an open interval I and a any point in I, and states that if F is defined by

$$F(x) = \int_a^x f(t)\,dt,$$

then

$$\begin{aligned} \frac{d}{dx}\int_a^x f(t)\,dt &= f(x) \\ F'(x) &= f(x) \end{aligned} \tag{C.2}$$

Defn C.1.3 (argmax)**.** The arguments to the *argmax* function are to be maximized by using their derivatives. You must take the derivative of the function, find critical points, then determine if that critical point is a global maxima. This is denoted as

$$\operatorname*{argmax}_x$$

C.2 Rules of Calculus

C.2.1 Chain Rule

Defn C.2.1 (Chain Rule)**.** The *chain rule* is a way to differentiate a function that has 2 functions multiplied together.

If

$$f(x) = g(x) \cdot h(x)$$

then,

$$\begin{aligned} f'(x) &= g'(x) \cdot h(x) + g(x) \cdot h'(x) \\ \frac{df(x)}{dx} &= \frac{dg(x)}{dx} \cdot g(x) + g(x) \cdot \frac{dh(x)}{dx} \end{aligned} \tag{C.3}$$

D Laplace Transform

Defn D.0.1 (Laplace Transform)**.** The *Laplace transformation* operation is denoted as $\mathcal{L}\{x(t)\}$ and is defined as

$$X(s) = \int\limits_{-\infty}^{\infty} x(t)e^{-st}dt \tag{D.1}$$