Cryptography 101: From Theory to Practice

Chapter 4 – Random Functions

Rolf Oppliger

February 7, 2022

Terms of Use

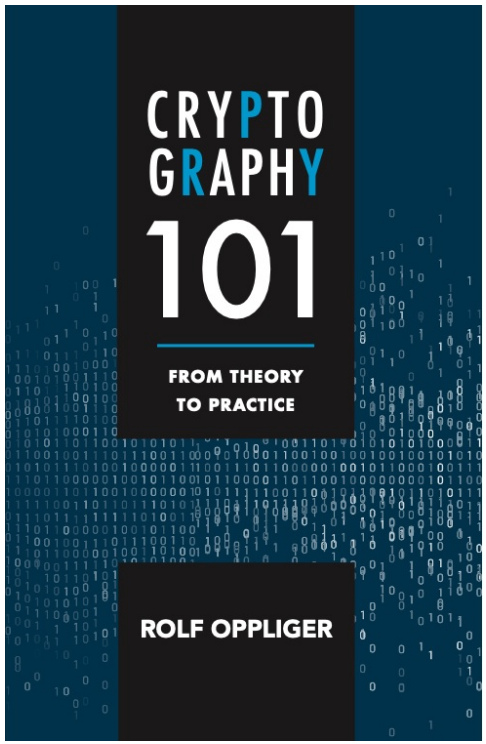
- This work is published with a CC BY-ND 4.0 license ()
  - CC = Creative Commons ()
  - BY = Attribution ()
  - ND = No Derivatives ()

whoami

rolf-oppliger.ch
rolf-oppliger.com

- Swiss National Cyber Security Centre NCSC (scientific employee)
- eSECURITY Technologies Rolf Oppliger (founder and owner)
- University of Zurich (adjunct professor)
- Artech House (author and series editor for information security and privacy)

Reference Book



ISBN 978-1-63081-846-3

`https://books.esecurity.ch/crypto101.html`

Challenge Me

Outline

4. Random Functions

4. Random Functions

4. Random Functions

4.1 Introduction

- A random generator outputs values that look random (i.e., it is characterized by its output)
- If one talks about random functions (or random oracles), then the focus is not the output of the function, but rather the way it is chosen
- According to Definition 2.2, a random function $f : X \to Y$ is chosen randomly from $\mathrm{Funcs}[X, Y]$
- There are $|Y|^{|X|}$ such functions, i.e., $|\mathrm{Funcs}[X, Y]| = |Y|^{|X|}$

4. Random Functions

4.1 Introduction

- If $X = Y$ and one only considers permutations of X, i.e., $\mathrm{Perms}[X]$, then a random permutation is chosen randomly from $\mathrm{Perms}[X]$
- There are $|X|!$ such permutations, i.e., $|\mathrm{Perms}[X]| = |X|!$
- Random functions and random permutations are purely theoretical constructs that are not meant to be implemented in practice

4. Random Functions

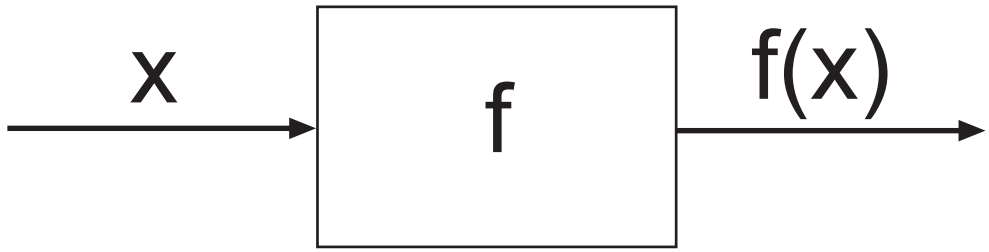
4.2 Implementation

- According to the way it is defined, a random function can output any value $y = f(x) \in f(X) \subseteq Y$ for $x \in X$
- The only requirement is that the same input value x must always map to the same output value y
- Except for that, everything is possible and does not really matter (for the function to be random)
- A random function can, for example, map all input values to the same output value

4. Random Functions

4.2 Implementation

- A random function is best thought of as a black box that has a particular input-output behavior
- This behavior can be observed by everybody



4. Random Functions

4.2 Implementation

- Another way to think about a random function f is as a large random table T with entries $T[x] = (x, f(x))$ for all $x \in X$
- The table can either be statically determined or dynamically generated (i.e., on the fly)
- In either case, implementing a random function is trivial
- However, one should not get too excited about this fact, because a random function doesn't serve any useful purpose (i.e., one cannot solve any real-world problem with a random function)

4. Random Functions

4.3 Final Remarks

- The sole purpose of this chapter is to introduce the notions of a random function and a random permutation
- Many cryptographic primitives and cryptosystems can be seen in this light
- They are not truly random but show a similar behavior and are thus indistinguishable from them
- To emphasize this subtle difference, such functions and permutations are called "pseudorandom"
- PRFs and PRPs are further addressed in Chapter 8

Questions and Answers

Thank you for your attention