Random Permutations

Notes on November 12 Reading

Jeffrey Goldberg
jeffrey@goldmark.org

November 12, 2021 (Updated May 8, 2024)

What is a PRP

Q What is a pseudo-random permutation (PRP)?

A A permutation that is indistinguishable from a truly random permutation

What is a PRP

Q What is a pseudo-random permutation (PRP)?

A A permutation that is indistinguishable from a truly random permutation

Permutations

A permutation is a the reordering of something. But we have to take it a little more abstractly

- A function
- The exact same set of things that are inputs of the function is the set of the outputs
- Each of the possible inputs and outputs must be "used" exactly once.

A reordering

Example: Reversing order

$$\begin{array}{rcr} 1 & \longrightarrow & 13 \\ 3 & \longrightarrow & 11 \\ 5 & \longrightarrow & 9 \\ 7 & \longrightarrow & 7 \\ 9 & \longrightarrow & 5 \\ 11 & \longrightarrow & 3 \\ 13 & \longrightarrow & 1 \end{array}$$

Figure: Reversing the order of some numbers. The set that is permuted is the set of numbers $\{3, 7, 9, 1, 11, 13, 5\}$. Each number appears exactly once on the left side of an arrow, and each number appears exactly once on the right side of an arrow.

A reordering

Example: a Ceasar cipher

A	$\longrightarrow$	D	J	$\longrightarrow$	M	S	$\longrightarrow$	V
B	$\longrightarrow$	E	K	$\longrightarrow$	N	T	$\longrightarrow$	W
C	$\longrightarrow$	F	L	$\longrightarrow$	O	U	$\longrightarrow$	X
D	$\longrightarrow$	G	M	$\longrightarrow$	P	V	$\longrightarrow$	Y
E	$\longrightarrow$	H	N	$\longrightarrow$	Q	W	$\longrightarrow$	Z
F	$\longrightarrow$	I	O	$\longrightarrow$	R	X	$\longrightarrow$	A
G	$\longrightarrow$	J	P	$\longrightarrow$	S	Y	$\longrightarrow$	B
H	$\longrightarrow$	K	Q	$\longrightarrow$	T	Z	$\longrightarrow$	C
I	$\longrightarrow$	L	R	$\longrightarrow$	U			

Figure: A Caesar cipher permutation: The set that is permuted is the set of letters ‘A’–‘Z’. Each letter appears exactly once on the left side of an arrow, and each letter appears exactly once on the right side of an arrow.

How many permutations are there?

If the set of things you are permuting has 7 things in it, there are $7 \times 6 \times 5 \times 4 \times 3 \times 2$ distinct permutations. This is written ‘7!’, and is read “seven factorial.” $7! = 5040$

$$26! \approx 2^{88}$$

We will be dealing with much larger numbers.

A keyed random permutation

Pick a permutation at random

Consider a function that take an input (a key) and randomly picks one of the 26! permutations of our set of 26 letters. It picks randomly and uniformly from that enormous set of permutations. But if you give you the same key you will get the same permutation.

A keyed psuedo-random permutation

Create a permutation

A PRP behaves just like a keyed truly random permutation, but

- It doesn't just pick a permutation completely at random.
- It efficiently generates an efficient permutation (remember that a permutation is a function)
- It can't be efficiently distinguished from a keyed truly random permutation

It behaves *as if* it is selecting a permutation at random.

A block cipher is a PRP

(we hope)

- Block ciphers work on “blocks”
- Blocks are like the letters of the alphabet in our previous example.
- For AES a block in any sequence of 128 bits
- For AES there are 2^{128} possible blocks.
- For AES there are 2^{128}! permutations. (note the factorial ‘!’).[1]

[1] The size of that number gives me the willies.

Three types

There are three ways to categorize block cipher modes

- Authenticated vs unauthenticated
- Counter vs chaining
- ECB