Schéma Cryptographique Probablement peu sûr

Sujet 7

One way function:

$$f_p : \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times \to \mathbb{Z}_{p^3}$$
$$(x, y) \mapsto x/y \bmod p^3$$

Parameters

$$p = \text{0xd2bf071417608219223ad076131586a9}$$
$$z = \text{0x4520670aac4c7f5af9f86bed585d6066dcb73b9ec8c9b885}$$
$$\text{36b46e252e64a1d28da6f8cf0d8bbf60fa6a4f8ee9854909}$$

Quick Reminders

The multiplicative group of integers modulo n, written $\mathbb{Z}_p^\times$, is the set of integers coprime to p from the set $\{0, 1, .., n-1\}$

Some examples

- $\mathbb{Z}_4^\times = \{1, 3\}$
- $\mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$

Problem

We start by determining if p is prime or not. It is indeed probably prime, according to a Miller-Rabin test with 100 trials.

Visualization

We can start playing around with the family of functions by using very simple visualizations. We do this to also get a feel for the geometric behavior of our function.

Number Theory

Implementation

This section discusses the implementation of Schema7 using Python.

Before we dive into writing code, we need to take a step back and carefully consider what the definition of f_p actually is. Deceptively simple, f_p presribes a division operation that takes place in some unspecified latent space, followed by a modulo operation.

`x / y`

We *interpret* the expression $x/y \bmod p^3$ as equivalent to:

$$x * y^{-1} \bmod p^3$$

where y^{-1} is the multiplicative inverse of y in $\mathbb{Z}_{p^3}^*$ and $*$ denotes traditional integer multiplication. In symbols, $y^{-1} * y \equiv 1 \bmod p^3$

Multiplicative Inverses

Given $y \in \mathbb{Z}_p^*$, there exists a unique $y^{-1} \in \mathbb{Z}_{p^3}^*$ such that $y^{-1} * y \equiv 1 \bmod p^3$. Furthermore, $y^{-1} = y^{p^3 - p^2 - 1} \bmod p^3$.

Proof

- Need to establish that y and p^3 are coprime for all y in p.
- By definition, y is coprime with p, p^3 has factors $p * p * p$, Thus $\gcd(y, p^3) = 1 \; \forall y \in \mathbb{Z}_{p^3}^*$.

- Thus, by Euler's theorem, $y^{\varphi(p^3)} \equiv 1 \bmod p^3$.
- Property of totient function $\varphi(p^3) = p^2\varphi(p) = p^2 * (p-1)$
- Then we have $y^{p^3-p^2} \equiv 1 \bmod p^3 \Leftrightarrow y * y^{p^3-p^2-1} \equiv 1 \bmod p^3$
- Thus, $y^{-1} = y^{p^3-p^2-1} \bmod p^3$.

Division

Analysis

We start our analysis by getting aquainted with the different operations and spaces present in this schema.

Domain, Codomain, Range

The domain of f_p is $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$ which has a cardinality of $(p-1)(p-1)$ for p prime. The codomain, $\mathbb{Z}_{p^3}$, has (p^3-1) elements. Trivially, f_p is not a surjective function as the codomain is a much larger space than the domain. Nor is f_p injective, as there exist multiple pairs of inputs that map to 1 (notably $x = y$).

Multiplicative Inverse

We can also analyze the implicit multiplicative inverse function and explicitize its domain and codomain.

Let $\text{inv}_{p^3}(y)$ denote the multiplicative inverse of $y \in \mathbb{Z}_{p^3}^*$. As a reminder, we define inv as:

$$\text{inv}_{p^3}(y) := y^{p^3-p^2-1} \bmod p^3$$

Let $Y_{p^3}^{-1}$ be the image of $\mathbb{Z}_p^*$ under inv_{p^3}. That is,

$$Y_{p^3}^{-1} := \left\{\text{inv}_{p^3}(y) \mid y \in \mathbb{Z}_p^*\right\}$$

Naturally, $Y_{p^3}^{-1} \subset \mathbb{Z}_{p^3}^*$ but the cardinality of this set of inverses is only $(p-1)$. We have this awkward situation where we only have the first $\sim\frac{1}{p^2}$ inverses of $\mathbb{Z}_{p^3}^*$

For example, for $p = 7$ we have $Y_{p^3}^{-1} = \{1, 172, 229, 86, 206, 286\}$

Visualization

We can develop some geometric intuition for the family f_p by visualizing our function with low p values.

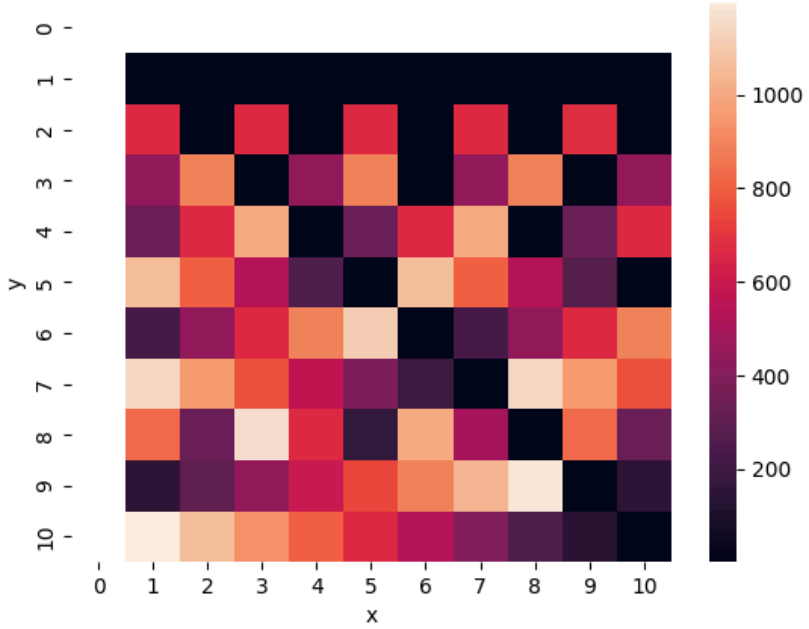


Figure 1: Heatmap of f_{11}

While this visualization can be misleading as we aren't able to distinguish between close values (for example, while all the values in the top row with $y = 1$ are actually different: {1, 2, ..., 11}, they appear to be the same hue), we are able to perceive global patterns in our function.

For starters, notice how all squares across the diagonal are pitch black. These values correspond to inputs where $x = y$, so we get $f_p(x, x) = x/x \bmod p^3 = 1$. Since the multiplicative inverse of 1 is itself, 1, we see a top row of $x/1 \bmod p^3 = x \bmod p^3$. Since $x \in \mathbb{Z}_p^*$ its magnitude never surpasses p^3 and the previous expression simplifies to x. Thus $f(x, 1) = x$.

In the second row ($y = 2$) we get some alternating pattern

On the left hand side with $x = 1$ we have the unadulterated multiplicative inverses of y.

Schwa7

We can study the family f_p through the lens of a hash function if we astutely apply a tranformation to our input in order to yield a series of $(x, y) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$.

We can conceive of a transformation in which we imagine breaking down the input value into a $(p - 1)$-radix number with two-digits. We assign x the value of the first digit + 1, and y the value of the second digit + 1.

Take for example the function f_5 and the input value 14. We split[1] 14 up into a 4-radix representation and get digits 3 and 2. Then, to project {0, 1, 2, 3} to our desired space $\mathbb{Z}_5^*$, we simply add one and end up with inputs $x = 4$ and $y = 3$.

binary	decimal	x	y	$f_5(x, y)$
0000	0	1	1	1

[1]We can use a combination of python's eucilidean division (// operator) and modulo (%) to represent any number with any base. For the case of two digits, we retrieve our first digit with x // p and our second digit with x % p.

binary	decimal	x	y	$f_5(x, y)$
0001	1	1	2	63
0010	2	1	3	42
0011	3	1	4	94
0100	4	2	1	2
0101	5	2	2	1
0110	6	2	3	84
0111	7	2	4	63
1000	8	3	1	3
1001	9	3	2	64
1010	10	3	3	1
1011	11	3	4	32
1100	12	4	1	4
1101	13	4	2	2
1110	14	4	3	43
1111	15	4	4	1

Note: We purposefully chose to have y vary before x so that the first $(p-1)$ values of our hash function are $f_p(1, y) = y^{-1} \bmod p$[3] which has far more unpredictability than changing x first and computing $f_p(x, 1) = x$.

The above enumeration of $\mathbb{Z}_p^* \times \mathbb{Z}_p^*$, while seemingly natural, is a completely arbitrary mapping. Any bijective permutation transforming our one-dimensional input $\{0, 1, ..., p^2 - 2p\}$[2] to the domain if f_p is suitable for implementing a hashing function with Schema 7 as its basis. However, not all enumerations are equal. In fact, as we have already mentioned, we chose to increment y before x in order to get more "randomness" for the first $p - 1$ inputs.

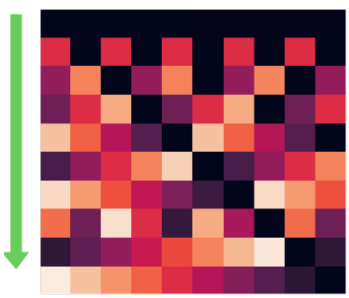
Such an enumeration would yield:

binary	decimal	x	y	$f_5(x, y)$
0000	0	1	1	1

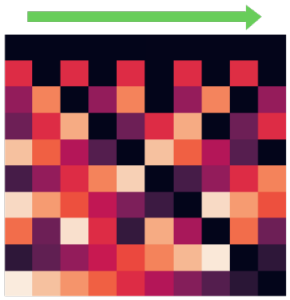
[2] $|\mathbb{Z}_{(p-1)(p-1)}| = (p^2 - 2p + 1)$ so the final element is $(p^2 - 2p + 1) - 1 = p^2 - 2p$

binary	decimal	x	y	$f_5(x, y)$
0001	1	2	1	2
0010	2	3	1	3
0011	3	4	1	4

Geometrically, the chosen enumeration traverses the 2 dimensional grid by descending along the left-hand side



incrementing y first



incrementing x first

,

Extending to variable-length input

The final step to implementing schema 7 as the hash function schwa7 is to open up the co-domain from a fixed input size to accepting inputs of any length.

To achieve this end, we apply a similar transformation as before and break down our input, $m \in \{0, 1\}^*$, into smaller, fixed-sized chunks. Only this time we break our input into as many subcomponents - base $p - 1$ digits - as needed.

Mathematically, we decompose:

$$\{0, 1\}^n \to \prod_i^k \mathbb{Z}_p^*$$

where n is the bit length of the input value and k is the number of $(p - 1)$-radix digits needed to represent our input. This is once again an arbitrary - albeit natural - transformation.

To avoid being overly formal, let's briefly examine a concrete example. Take $p = 5$ and let's use an input value of 17. With 4 as our radix, we have:

$$17 = 1 * 4^2 + 0 * 4^1 + 1 * 4^0$$

As before, we add 1 to each base-$(p - 1)$ digit in order to yield a sequence of values in $\mathbb{Z}_p^*$:

$$17 \mapsto [2, 1, 2]$$

All that's left to do is condense the sequence of $m_i \in \mathbb{Z}_p^*$ into a single value. Consider the following condensing function:

$$\varphi : \mathbb{Z}_p^* \times \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$
$$(x, y) \mapsto \big(f_p(x, y) \bmod p - 1\big) + 1$$

We can use repeated calls to φ in order to combine the elements of our sequence, internally using f_p as our indexing function. We perform this reduction with the following recursive function:

1. For input $m = [m_0, m_1, ..., m_{k-1}, m_k]$, reduce m using repeated applications of φ:

input: $m = [m_0, m_1, ..., m_{k-1}, m_k]$

$[m_0, m_1, ..., \varphi(m_{k-1}, m_k)]$
2.