1 Introduction

We provide here a slightly simplified description of an existing cryptosystem. For reasons related to challenge design[1] *we leave it nameless here.*

We have found a description of a cryptographic scheme the aliens left behind after stealing all our RuneScape gold. They also left behind a single ciphertext, containing our flag. Unfortunately, we couldn't recover the source code, but we're fairly sure it was encrypted with this scheme.

Our forensic engineers say they managed to even recover a large part of the private key for this flag, so maybe that can help you out too.

2 Cryptosystem

Let $\mathbb{F}$ be a finite field of characteristic 2 and order q. That is: $\mathbb{F} = \mathbb{F}_q$ with $q = 2^k$ for some k.
We define $\mathbb{K}$ to be a degree n extension of $\mathbb{F}$, represented by polynomials from $\mathbb{F}[X]/(P)$ where P is a degree n irreducible polynomial over $\mathbb{F}$. Any extension ring, and as such $\mathbb{K}$, can also be seen as an $\mathbb{F}$-vector space $\mathbb{V} = \mathbb{F}_q^n$.
To make this correspondence explicit, we introduce the basis $(\beta_i)_{0 \leq i < n}$ for $\mathbb{V}$ as $\beta_i = X^i$. This allows us to introduce the $\mathbb{F}$-linear conversion maps

$$\phi : \mathbb{K} \to \mathbb{V} : a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} \mapsto (a_o, a_1, \ldots, a_{n-1})$$

and

$$\phi^{-1} : \mathbb{V} \to \mathbb{K} : (a_0, a_1, \ldots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i \beta_i.$$

As a note on notation: a value x will be denoted with either $\bar{x} \in \mathbb{V}$ or $\mathbf{x} \in \mathbb{K}$.
The key idea to this cryptosystem is that we want the public key to be a function f that is hard to invert, while the private key contains a decomposition of f into separately invertible parts. Knowing this decomposition then allows us to invert the entire function, as

$$(f_0 \circ f_1 \circ \cdots \circ f_n)^{-1} = f_n^{-1} \circ \cdots \circ f_1^{-1} \circ f_o^{-1}.$$

In this case, we will construct f out of 3 pieces that work over either $\mathbb{K}$ or $\mathbb{V}$, and glue those together by application of ϕ and ϕ^{-1}.
The first and last of our 3 components will be denoted as L_1 and L_2, respectively. These are both $\mathbb{F}$-affine maps working over $\mathbb{V}$. That is, we can represent L_i as the pair $(M_i, \bar{k_i}) \in \mathbb{F}_q^{n \times n} \times \mathbb{F}_q^n$ such that M_i is invertible over $\mathbb{F}_q$. The map L_i itself will then be

$$L_i : \mathbb{F}_q^n \to \mathbb{F}_q^n : \bar{x} \mapsto M_i x + \bar{k_i}.$$

[1] i.e. we don't want you to try and find another implementation or attack right away, but rather follow along what we present here

L_1 and L_2 are part of the decomposition trapdoor, and should as such be considered private.
In between the application of L_1 and L_2, we will apply the monomial map ψ. Here, we work over $\mathbb{K}$, choose the simple function

$$\psi : \mathbb{K} \to \mathbb{K} : \mathbf{u} \mapsto \mathbf{u}^h$$

where we let $h = q^\theta + 1$ be another private variable, subject to ψ^{-1} existing.
Putting it all together, we obtain the public key

$$f : \mathbb{V} \to \mathbb{V} = L_2 \circ \phi \circ \psi \circ \phi^{-1} \circ L_1$$

and the private key

$$(h, M_1, k_1, M_2, k_2).$$

To represent and transmit the public key f, we can evaluate it on the symbolic variable $\bar{x} = (x_0, \ldots, x_{n-1})$ as $\bar{y} = f(\bar{x})$ and obtain a set of n equations $y_i = f_i(\bar{x})$ over $\mathbb{F}$. To encrypt the plaintext $\bar{x}$, we simply evaluate $\bar{y} = f(\bar{x})$ by way of evaluating each individual f_i in the public key. The ciphertext consists simply of $\bar{y}$.

3 Sample

As an example of this derivation of the public key, we consider some toy parameters. We set $q = 2^2$, $n = 3$ and $h = 17$. α is an element of $\mathbb{F} = \mathbb{F}_{2^2}$ such that $\alpha^2 = \alpha + 1$. The extension $\mathbb{K}$ is the nth degree extension of $\mathbb{F}$, modulo the polynomial $X^3 + \alpha$.

$$M_1 = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 0 & \alpha+1 \\ \alpha & \alpha & \alpha \end{bmatrix} \qquad k_1 = (1, \alpha, 1)$$

$$M_2 = \begin{bmatrix} 1 & \alpha & \alpha+1 \\ 0 & 1 & \alpha+1 \\ \alpha & \alpha & \alpha+1 \end{bmatrix} \qquad k_2 = (\alpha+1, 0, \alpha+1)$$

Now consider the symbolic variable $\bar{x} = (x_0, x_1, x_2)$, we can compute

$$\bar{y}(\bar{x}) = L_2(\phi(\psi(\phi^{-1}(L_1(\bar{x}))))),$$

resulting in

$$\begin{aligned} \bar{y}(x_0, x_1, x_2) &= (y_0, y_1, y_2) \\ y_0 &= x_0^2 + \alpha^2 x_0 x_1 + \alpha^2 x_1^2 + \alpha x_0 x_2 + \alpha^2 x_1 x_2 + \alpha^2 x_2^2 + x_0 + \alpha x1 + \alpha \\ y_1 &= x_0^2 + \alpha^2 x_0 x_1 + \alpha x_1^2 + \alpha^2 x_0 x_2 + x_1 x_2 + \alpha x_2^2 + \alpha x_0 + \alpha^2 x_1 + \alpha^2 \\ y_2 &= \alpha x_0^2 + \alpha^2 x_0 x_1 + \alpha^2 x_1^2 + \alpha^2 x_0 x_2 + \alpha x_1 x_2 + \alpha x_0 + x_1 + \alpha^2 \end{aligned}$$

As a sanity check, here are some intermediate values:

$$(L_1(\bar{x}))_0 = x_0 + \alpha * x_2 + 1$$
$$\phi(\psi(\phi^{-1}(L_1(\bar{x}))))_1 = \alpha x_0^2 + \alpha x_1^2 + x_0 x_2 + \alpha^2 x_0$$

4 Instantiation

For this challenge, $q = 2^8$ and $\mathbb{F} = \mathbb{F}_q$ is represented as the quotient

$$\mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X^2 + 1).$$

α is a primitive element of $\mathbb{F}$ such that $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$. $\mathbb{K}$ is the 60th degree extension of $\mathbb{F}$ modulo the polynomial provided in `output.txt`.
To embed a binary message of length n into $\mathbb{V}$, we place a byte in each component. A byte $\sum b_i 2^i$ can be represented as $\sum b_i \alpha^i$.