RIJNDAEL CIPHER

MATH 195

For any cryptographic system, we need to define encryption and decryption functions

$$\begin{aligned} E, D &: \mathcal{K} \times \mathcal{P} \to \mathcal{C} \\ E &: (k, x) \mapsto E_k(x) \\ D &: (k, x) \mapsto D_k(x) \end{aligned}$$

such that $D_k E_k = \mathrm{id}_{\mathcal{P}}$, so that these are inverse to each other. Recall $\mathcal{K}$ is the key space, $\mathcal{P}$ is the plaintext message space, and $\mathcal{C}$ is the ciphertext message space.

We take $\mathcal{P} = \mathcal{C}$ equal to the *state space* $\mathcal{S} = \mathbb{F}_2^{32N_b}$, where

$$N_b = \{4, 6, 8\},$$

and we shall take $N_b = 4$ so that $\mathcal{S} = \mathbb{F}_2^{128}$. This is to say, $\mathcal{S}$ is a 128-dimensional vector space over $\mathbb{F}_2$, or put another way, it consists of bit strings of length 128. Similarly, the key space is $\mathbb{F}_2^{32N_k}$ where $N_k \in \{4, 6, 8\}$; we will take $N_k = 4$ as well.

The letters $\tau_s, \sigma, \beta, \mu$ are permutations of $\mathcal{S}$ from which E_k and D_k are built up.

For each $s \in \mathcal{S}$, the function

$$\tau_s : \mathcal{S} \to \mathcal{S}$$

is defined by

$$\tau_s(x) = x + s;$$

hence τ_s is 'translation by s', called the AddRoundKey transformation.

A *state* (an element of $\mathcal{S}$) is pictured as a $4 \times N_b$ matrix with entries that consist of 1 byte (8 bits) each, e.g.

$$\begin{pmatrix} 01010010 & 01001100 & 10101011 & 01110010 \\ 01010101 & 11010101 & 11111111 & 00110100 \\ 11011010 & 10110101 & 11010001 & 10111011 \\ 10111010 & 10111101 & 01110110 & 00000001 \end{pmatrix}$$

where we read the bytes from top to bottom, then left to right:

$$01010010\ 01010101\ 11011010\ \ldots\ 10111011\ 00000001$$

in the above example. (Recall $N_b = 4$.) The set of all bytes is $\mathbb{F}_2^8$, and it is identified with the field

$$\mathbb{F}_{256} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1),$$

by identifying $(b_7 b_6 \ldots b_1 b_0)$ with the polynomial

$$b_7 X^7 + b_6 X^6 + \cdots + b_1 X + b_0 \in \mathbb{F}_{256}.$$

This gives us a multiplication on 8 bit strings. Therefore $\mathcal{S}$ is now the set of 4×4 matrices with entries from $\mathbb{F}_{256}$.

This is some of the material covered April 2–4, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight jvoight@math.berkeley.edu.

The map $\beta : \mathcal{S} \to \mathcal{S}$ is called the $\mathsf{ByteSub}$ transformation, and it is defined by

$$\beta \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} = \begin{pmatrix} B(a_{0,0}) & \dots & B(a_{0,3}) \\ \vdots & \ddots & \vdots \\ B(a_{3,0}) & \dots & B(a_{3,3}) \end{pmatrix}.$$

where $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ is some dreadful permutation to be defined later.

The map $\sigma : \mathcal{S} \to \mathcal{S}$ is the $\mathsf{ShiftRow}$ transformation: σ shifts the ith row ($i = 0, 1, 2, 3$) cyclically by i positions to the left:

$$\sigma \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} = \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{pmatrix}.$$

In other words,

$$\sigma((a_{i,j}))_{i,j=0,\dots,3}) = (a_{i,i+j \bmod 4})_{i,j=0,\dots,3}.$$

The map $\mu : \mathcal{S} \to \mathcal{S}$ is the $\mathsf{MixColumn}$ operation defined by

$$\mu \begin{pmatrix} | & | & | & | \\ a_0 & a_1 & a_2 & a_3 \\ | & | & | & | \end{pmatrix} = \begin{pmatrix} | & | & | & | \\ Ma_0 & Ma_1 & Ma_2 & Ma_3 \\ | & | & | & | \end{pmatrix}$$

where a_i are vectors, $a_i \in \mathbb{F}_{256}^4$, and where $M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$ is a linear map (over $\mathbb{F}_{256}$, so M can be given by a 4×4 matrix with coefficients from $\mathbb{F}_{256}$).

The definition of M: identify $\mathbb{F}_{256}^4$ (the *word space*: 1 byte is 8 bits, 1 word is 4 bytes, 1 state is N_b words) with $\mathbb{F}_{256}[Y]/(Y^4+1)$. The elements of $\mathbb{F}_{256}[Y]/(Y^4+1)$ are represented by polynomials $b_3Y^3 + b_2Y^2 + b_1Y + b_0$, where $b_i \in \mathbb{F}_{256}$. Define

$$M : \mathbb{F}_{256}[Y]/(Y^4+1) \to \mathbb{F}_{256}[Y]/(Y^4+1)$$

by

$$M(w) = c \cdot w \pmod{Y^4+1}$$

where

$$c = \mathtt{03}Y^3 + \mathtt{01}Y^2 + \mathtt{01}Y + \mathtt{02} \in \mathbb{F}_{256}[Y]/(Y^4+1)$$

where $\mathtt{03} = 00000011 = X + 1$ in $\mathbb{F}_{256}$, and similarly $\mathtt{01} = 00000001 = 1 \in \mathbb{F}_{256}$, $\mathtt{02} = 00000010 = X \in \mathbb{F}_{256}$.

Note that $c(1) = 1$, so since $Y^4 + 1 = 0$, $c^4 = 1$.

The key space $\mathcal{K} = \mathcal{S}$. Key expansion transforms a given key $k \in \mathcal{K}$ into a sequence $k_0(= k), k_1, \dots, k_{10}$ "round key" that belong to $\mathcal{S}$, to be explained.

The formula for E_k, given as maps, is:

$$E_k = \tau_{k_{10}}\sigma\beta\tau_{k_9}\mu\sigma\beta \dots \tau_{k_2}\mu\sigma\beta\tau_{k_1}\mu\sigma\beta\tau_{k_0}.$$

Notice that we do not have a final application of μ: since μ is a known map, the additional application would be wasteful, as μ and τ commute ($\mu\tau_s = \tau_{\mu(s)}\mu$) any cryptanalyst could easily undo this map.

To decrypt, we apply the inverse of these maps in the opposite order, using commutation relations:

$$D_k = E_k^{-1} = \tau_{k_0}\sigma^{-1}\beta^{-1}\tau_{\mu^{-1}(k_1)}\mu^{-1}\sigma^{-1}\beta^{-1}\tau_{\mu^{-1}(k_2)}\mu^{-1} \dots \tau_{\mu^{-1}(k_9)}\mu^{-1}\sigma^{-1}\beta^{-1}\tau_{k_{10}}.$$

Note that there would be asymmetry in the application of the maps if we applied an additional μ to conclude E_k, as we would then have to apply μ^{-1} at the beginning of D_k.

There are two maps still left to define. First, we define $A : \{f \in \mathbb{F}_2[X] : \deg f < 8\}$ to itself by

$$A(f) \equiv (X^4 + X^3 + X^2 + X + 1)f + (X^6 + X^5 + X + 1) \pmod{X^8 + 1}.$$

Note that in $\mathbb{F}_2[X]$, $X^8 + 1$ is not irreducible, so $\mathbb{F}_2[X]/(X^8 + 1)$ is *not* a field! Indeed, by the freshperson's dream $X^8 + 1 = (X + 1)^8$. (We say 'A' for affine, since it is a homomorphism followed by a translation.)

In fact, A^4 is the identity map, $A^{-1} = A^3$, and

$$A^{-1}(f) \equiv (X^6 + X^3 + X)f + (X^2 + 1) \pmod{X^8 + 1}.$$

Define $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ by

$$B(a) = \begin{cases} A(a^{-1}), & a \neq 0, a^{-1} \text{ computed in } \mathbb{F}_{256}; \\ A(0), & a = 0. \end{cases}$$

Note: $B(a) = A(a^{254})$, where a^{254} is computed in $\mathbb{F}_{256}$, and B is the composition of A and the 'inversion' map. This is the only nonlinear ingredient in the entire scheme.

Finally, we must give key expansion: Given a key $k \in \mathcal{K} = \mathcal{S}$, we produce 11 round keys $k_0, \dots, k_{10} \in \mathcal{S}$. Write

$$k = \begin{pmatrix} | & | & | & | \\ w_0 & w_1 & w_2 & w_3 \\ | & | & | & | \end{pmatrix}$$

We expand k into

$$k = \begin{pmatrix} | & | & | & | & & | & | & | \\ w_0 & w_1 & w_2 & w_3 & \dots & w_{41} & w_{42} & w_{43} \\ | & | & | & | & & | & | & | \end{pmatrix}$$

so that

$$k_i = \begin{pmatrix} | & | & | & | \\ w_{4i} & w_{4i+1} & w_{4i+2} & w_{4i+3} \\ | & | & | & | \end{pmatrix}$$

where

$$w_j = \begin{cases} w_{j-1} + w_{j-4}, & j \not\equiv 0 \pmod 4, \\ \gamma(w_{j-1}) + w_{j-4}, & j \equiv 0 \pmod 4, \end{cases}$$

and

$$\gamma \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} B(b) \\ B(c) \\ B(d) \\ B(a) \end{pmatrix} + \begin{pmatrix} X^{(j-4)/4} \bmod m(X) \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

and $m(X) = X^8 + X^4 + X^3 + X + 1$.

In fact, $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ for all $a \in \mathbb{F}_{256}$ one has

$$B(a) = \mathtt{63} + \mathtt{8f}a^{127} + \mathtt{b5}a^{191} + \mathtt{01}a^{223} + \mathtt{f4}a^{239} + \mathtt{25}a^{247} + \mathtt{f9}a^{251} + \mathtt{09}a^{253} + \mathtt{05}a^{254}$$

where the coefficients are written in hexadecimal (e.g. `63`=01100011). Note that this has all 9 terms (there is no easy algebraic relation).