T-79.4502 Cryptography and Data Security
T-110.5210 Cryptosystems
December 15, 2011 / Exam

Each problem is worth 6 points. This is a 30 point exam. A non-programmable pocket calculator is allowed.

1. Set $\mathbf{F}_{2^3} \cong \mathbf{F}_2[x]/(x^3+x^2+1)$. Consider a bijective S-box $S : \mathbf{F}_{2^3} \to \mathbf{F}_{2^3}$ such that

$$S(a) = b \Leftrightarrow b = g(f(a))$$

where $f : \mathbf{F}_{2^3} \to \mathbf{F}_{2^3}$ is

$$f(t) = u \Leftrightarrow u = \begin{cases} 0 & \text{if } t = 0, \\ t^{-1} & \text{otherwise,} \end{cases}$$

and $g : \mathbf{F}_{2^3} \to \mathbf{F}_{2^3}$ by

$$g(u) = v \Leftrightarrow \vec{v} = Y\vec{u} + \vec{z} \text{ where}$$

$$Y = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \vec{z} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

and $\vec{a}$ denotes $a \in \mathbf{F}_{2^3}$ as a vector in $\mathbf{F}_2^3$, e.g., if $a = x + x^2$ then $\vec{a} = (0, 1, 1)$. This construction is analogous to that of AES but with a smaller field and different constants. Give S as a lookup table, i.e., compute the output of S for all possible inputs.

2. Consider the linear recursive sequence $s_i = s_{i-1} + s_{i-4}$ over $\mathbf{F}_2$.

   (a) Draw a block diagram of a 4-stage LFSR that implements this sequence.

   (b) Set the initial state as $s_0 = 1$ and $s_1 = s_2 = s_3 = 0$. Calculate the sequence output until it becomes periodic.

   (c) Calculate the periods of the sequence for all possible initial states.

3. Recall that the SHA-1 hash function uses a Davies-Meyer style compression function such that $H_i = E_{m_i}(H_{i-1}) \boxplus H_{i-1}$ where $H_0 = IV$, $E_K(x)$ is encryption of 160-bit x under 512-bit key K using a dedicated block cipher, and $\boxplus$ is vector addition with components added in $\mathbf{Z}_{2^{32}}$. Consider a variant where the chaining values are computed instead as $H_i = E_{m_i}(H_{i-1})$. Give a method to compute preimages with complexity $O(2^{80})$ (i.e., roughly 2^{80} steps).

4. Consider the RSA cryptosystem with modulus $n = 31 \cdot 43 = 1333$.

   (a) Compute the private decryption exponent d using public encryption exponent $e = 257$.

   (b) Encrypt the plaintext $p = 32$.

   (c) Decrypt the ciphertext $c = 44$.

5. Consider Diffie-Hellman key exchange in $\mathbf{F}_2[x]/(x^4+x+1)$ with multiplicative generator $g = x$.

   (a) In the first protocol run, Alice's secret exponent is $a = 8$ and Bob's secret exponent $b = 7$. Compute the shared key K.

   (b) In the second protocol run, Alice sends $\alpha = x^3 + x^2 + 1$ for her public key. Compute the discrete logarithm of α to the base g.

Feedback from students plays a vital role in improving this course. Please submit any feedback by following the link through the course Noppa page.