TIE-31106 Cryptography Engineering
21 Dec 2016 / Exam

Tampere University of Technology
B. B. Brumley

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

1. Consider the Cipher Block Chaining (CBC) mode used with AES-128.
   (a) Draw a block diagram for CBC encryption.
   (b) After observing k sequential CBC ciphertext blocks $C_1 \ldots C_k$, an attacker notices $C_j = C_k$ for some $j < k$. Assuming the attacker also knows plaintext block M_k, show how to recover M_j.
   (c) Estimate the smallest k for which the above attack succeeds with probability greater than one half.
2. Consider Double DES that, with 56-bit key K_1 and 56-bit key K_2, encrypts 64-bit plaintext P to 64-bit ciphertext C using $C = E_{K_2}(E_{K_1}(P))$ where E is DES encryption. Given a known plaintext/ciphertext pair (P, C), show how to recover (K_1, K_2) using roughly 2^{56} steps with the meet-in-the-middle technique.
3. 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.
4. Consider the RSA cryptosystem with modulus $n = 17 \cdot 59 = 1003$.
   (a) Compute the private decryption exponent d using public encryption exponent $e = 3$.
   (b) Encrypt the plaintext $p = 58$.
   (c) Decrypt the ciphertext $c = 16$.
5. Consider Diffie-Hellman key exchange in $\mathbf{F}_{29}^*$ with multiplicative generator $g = 2$.
   (a) In the first protocol run, Alice's secret exponent is $a = 13$ and Bob's secret exponent $b = 9$. Compute the shared key K.
   (b) In the second protocol run, Alice sends $\alpha = 27$ for her public key. Compute the discrete logarithm of α to the base g.