Problem Set 5 – Due Wed, 13 Feb 2019 at 12pm

Problem 14. Bob proposes a 128-bit blockcipher, Tango32, that works like this. It has 16 S-boxes, $S_1, \ldots, S_{16}$, each a permutation mapping 8-bits to 8-bits. It uses a 128-bit key that gets mapped into 32 subkeys, $K_1, \ldots, K_{32}$, each 128 bits. To encrypt an input block $X$, for each of 32 rounds $i$, the cipher:

1. Replace $X$ by $X \oplus K_i$;
2. Replace the $j$-th byte of $X$, $X[j]$, by $S_j[X[j]]$ (for each $1 \leq j \leq 16$);
3. Circularly rotate $X$ by $c_i$ byte position to the left, $X \leftarrow X \lll (8c_i$, where $c_i \in [0..15]$.

The ciphertext is the final value of $X$.

Bob has carefully designed Tango32’s S-boxes, key schedule, and rotation constants.

Break Bob’s design using at most a few hundred plaintext/ciphertext pairs. Your break should be so bad that you can subsequently decrypt anything that’s encrypted with the same key.

Problem 15. CBC-Chain is a stateful blockcipher-based mode of operation. To encrypt, we use CBC with an IV that is the last ciphertext block produced from the prior encryption. Initially, the IV is a random string.

Part A. Formally define key generation, encryption, and decryption for CBC-Chain $E$ given a blockcipher $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$.

Part B. Show that CBC-Chain $E$ is never IND-secure by giving a devastating, efficient attack on it.

Problem 16. Can a blockcipher $E: \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$ be secure as a PRP if it has the following characteristics? Briefly justify each answer. Where necessary, interpret numbers as 128-bit strings.

Part A. The first bit of $E_K(X)$ doesn’t depend on the last bit of $X$.

Part B. The first bit of $E_K(X)$ doesn’t depend on the last bit of $K$.

Part C. $\bigoplus_{i=1}^{10} E_K(i) = 0$.

Part D. $E_K^{-1}(0) = E_K(1)$.

Part E. $E_K(K) = K$. 