CS 427 Homework 1

Robert Detjens

---

1. Given the two ciphertexts below, are they `alpha`/`bravo` or `delta`/`gamma`? What was the key?

- c1 = `0011010000111100011000011011000101100100`
- c2 = `0011011100111000011000001010100001100100`

c1 is `delta` and c2 is `gamma`. Key is `01010000001011001000011011100010100000101`.

$$c_1 \oplus \text{'alpha'} \oplus c_2 \neq \text{'bravo'}$$
$$c_1 \oplus \text{'delta'} \oplus c_2 = \text{'gamma'}$$

2. Show that non-mod-2 addition is not uniformly distributed.

With mod-2 addition (XOR), a plaintext input of 0^λ will generate a ciphertext somewhere in the range of $\{0,1\}^\lambda$, and a plaintext of 1^λ will also generate a ciphertext in $\{0,1\}^\lambda$, as expected.With normal addition, a plaintext input of 0^λ still generates a ciphertext somewhere in the range of $\{0,1\}^\lambda$, and a plaintext of 1^λ will instead generate a ciphertext in $\{1,2\}^\lambda$.

$$TEST(0^\lambda) \in \{0,1\}^\lambda$$
$$TEST(1^\lambda) \in \{1,2\}^\lambda$$

Examining the ciphertext probability, the probability that both of these plaintext inputs will generate the same key – e.g. $c = 0^\lambda$ – should be $\frac{1}{3^\lambda}$ as there are 3 possible digits in the search space. However, while the actual probability of $c = 0^\lambda$ occuring for $TEST(0^\lambda)$ is $\frac{1}{2^\lambda}$, the probability of $TEST(1^\lambda)$ generating that same c is 0 – it cannot happen. Thus, the distribution of ciphertexts that $TEST()$ generates is not uniformly distributed for all inputs.

3. Show that bitwise AND is not uniformly distributed.

With mod-2 addition (XOR), a plaintext input of 0^λ will generate a ciphertext somewhere in the range of $\{0,1\}^\lambda$, and a plaintext of 1^λ will also generate a ciphertext in $\{0,1\}^\lambda$, as expected. With bitwise AND, a plaintext input of 0^λ instead always generates a ciphertext of 0^λ, and a plaintext of 1^λ will generate a ciphertext always equal to the key.

Thus, the distribution of ciphertexts that $TEST()$ generates with bitwise AND depends on the input plaintext and is not uniformly distributed across $\{0,1\}^\lambda$.

$$TEST(0^\lambda) = 0^\lambda$$
$$TEST(1^\lambda) \in \{0,1\}^\lambda$$

Examining the ciphertext probability, the probability that both of these plaintext inputs will generate the same key – e.g. $c = 0^\lambda$ – should be $\frac{1}{2^\lambda}$ as there are 2 possible digits in the search space. However, while the actual probability of $c = 0^\lambda$ occuring for $TEST(1^\lambda)$ is $\frac{1}{2^\lambda}$, the probability of $TEST(0^\lambda)$ generating that same c is 1 – it always happens. Thus, the distribution of ciphertexts that $TEST()$ generates is not uniformly distributed for all inputs.