6.857 Homework	**Problem Set 3**	# 3-2 Stream Ciphers
Julia Huang		
Skanda Koppula		
Kimberly Toy		March 23, 2015

This problem took approximately 15 man-hours.

For convenience, the four constructions have been re-stated here:
A. $x_i = f(i)$
B. $x_i = f(x_{i-1}) \oplus i$
C. $x_i = f(x_{i-1} \oplus i)$
D. $x_i = f(x_{i-1} \oplus i) \oplus i$

The three constructions that have constant quality $\theta(1)$ are A, C, and D, while construction B has a quality of $\theta(\sqrt{2^n})$

To prove the $\theta(1)$ bound on A, C, and D, we will present mappings for f and starting values for x_0 that will result in all values of x_i being the same.

Construction A: Let $f(i) = 0$ for any i and for any starting value of x_0. This will trivially cause all values of x_i to equal 0.
Construction C: Again, let $f(i) = 0$ for any i and for any starting value of x_0. Because x_i is the result of f applied to some value, this will cause all values of x_i to equal 0.
Construction D: Let $f(i) = i$ and $x_i = 0$. The first value, x_1 will equal zero, as shown:

$$x_1 = f(x_0 \oplus i) \oplus i$$

$$x_1 = f(0 \oplus i) \oplus i$$

$$x_1 = f(i) \oplus i = i \oplus i = 0$$

This same logic can be used to show that all values of x_i would equal 0.

For **construction B**, we will demonstrate a mapping f that achieves $\theta(\sqrt{2^n})$ quality and then show that a lower quality cannot be achieved. The idea behind this construction is to "mask" half of the bits in each number, or set those bits equal to zero. This scheme would reduce 2^n unique n-bit numbers into only $\sqrt{2^n}$ unique numbers.

Given B's construction, the portion $f(x_{i-1})$ will operate as a mask, which will be applied to i. As it is difficult to create a mapping f that will consistently mask either only the first $n/2$ bits of i or only the second $n/2$ bits, we will create a scheme that alternately masks out the first and second halves of the bit strings. This will result in $2 * \sqrt{2^n}$ unique numbers, which is still within the $\theta(\sqrt{2^n})$ bound.

Knowing that each result, x_i should have either the first $n/2$ bits or second $n/2$ equal to zeroes due to our masking scheme, we only need to construct a mapping f for bit strings in those forms: $s \mid\mid n/2\ zeroes$ or $n/2\ zeroes \mid\mid s$, where s is any bit string of length n/2. In order to create our alternating mask, we will define the mapping f as follows:

$$f(n/2\ zeroes \mid\mid s) = s \mid\mid n/2\ zeroes$$

$$f(s \mid\mid n/2\ zeroes) = n/2\ zeroes \mid\mid (s+1)$$

where if $s+1$ overflows $n/2$ bits, the top-most bit will be cut off. Let $x_i = 0$. This function of f guarantees that top half of the next number i will be masked out by the portion s or the lower half by $s+1$, and as stated earlier, this meets the $\theta(\sqrt{2^n})$ bound.

Proof of $\sqrt{2^n}$ lower bound: In order to create a mapping f, such that there are fewer than $\theta(\sqrt{2^n})$ unique x_i, we would need to create a scheme that masks more than $n/2$ bits of each number i. We will prove that it is impossible to create such a scheme.

Let m be some integer greater than $n/2$ that represents the number of bits that our scheme can mask. In order for the mask to change m bits of each i into zeroes, the mask has to replicate m bits of i.

The number of possible x_i that can be outputted is 2^{n-m} because the result must have at least m zeroes. The number of unique masks, or outputs of $f(x_{i-1})$, needed to implement the outlined scheme is 2^m. Because each x_i becomes an input for $f(x_{i-1})$, we can see that this scheme would require f to map 2^{n-m} inputs to 2^m outputs. As $m > n/2$, it follows that $2^m > 2^{n-m}$, which shows that f is an impossible mapping.

Therefore, construction B has a quality of $\theta(\sqrt{2^n})$.