Manual:: Operation Deep Magic: Cryptanalysis

Henry Ng

1013133, Vancouver BC V5P2Y6, Canada info@henryng.org

1 Probability

The number of occurences of A divided by the number of experiments performed is the proportion of times A occurs. The expected proportion of occurences is the probability of A. $P(A)$ is any number $0 \leq P(A) \leq 1$, where 0 indicates impossibility and 1 indicates certainty. P of A or the **probability of** A is written as

$$P(A) = \frac{\text{number of ways } A \text{ can occur}}{\text{total number of possible outcomes}}$$

P of A in base 2 scientific notation is written as

$$P(A) = 2^{\log_2 P(A)} = 2 * *(\log_2 P(A))$$

Probability bias of A plus 0.5 in scientific notation is written as

$$P(A) = \begin{cases} 0.5 + 10^{\log_{10}(P(A)-0.5)} \text{ or } 0.5 + 2^{\log_2(P(A)-0.5)}, \text{if } P(A) \geq 0.5 \\ 0.5 - 10^{\log_{10}|P(A)-0.5|} \text{ or } 0.5 - 2^{\log_2|P(A)-0.5|}, \text{if } P(A) < 0.5 \end{cases}$$

2 Combinatorics

An ordered arrangement of r elements selected from a set of n elements is a **permutation** of n elements taken r at a time. A collection of r elements, regardless of order, selected from a set of n elements is called a **combination** of n elements taken r at a time.

3 Logical Operators

The result of b_1 exclusive-or b_2 is 1 if only one of the bits is 1 and otherwise is 0 if both are the same bit, is written as

$$b_1 \oplus b_2 = b_1 \mathbf{XOR} b_2$$

The result of b_1 inclusive-or b_2 is 1 if any one of the bits is 1 and otherwise is 0 if both are 0, is written as

$$b_1 \vee b_2 = b_1 \mathbf{OR} b_2$$

The result of b_1 logical-and b_2 is 1 if both of the bits is 1 and otherwise is 0, is written as

$$b_1 \wedge b_2 = b_1 \mathbf{AND} b_2$$