Nirbhay Sharma (B19CSE114)

Assignment-2 - Cryptography

1.a

Given:

$$G(s) : [0,1]^m \rightarrow [0,1]^n : m < n$$

$1 + 2$

$G(s) : [0,1]^m \rightarrow [0,1]^n : m < n$

$\wedge$

$\oplus$

$\geq$

1.b

1.c

1.d

$$[0,1]^m \rightarrow [0,1]^n$$

$$[0,1]^n$$

$Pr[D(r) = 1] = \frac{2^n}{2^{2n}} = \frac{1}{2^{3n}}$

so $|Pr[D(G_4(s)) = 1] - Pr[D(r) = 1]| = |1 - \frac{1}{2^n}| > \epsilon$

$\sum_1^2 (t_i + x_i) = 5 + 1$

$(x + y)\ [x + y]\ \{x + y\}\ \langle x + y \rangle\ |x + y|\ |x + y|$

$1 \& 2$

$1 + 2$

$$\{x_t + y_t\} \textunderscore k_t$$