Block cipher is intended to resemble a random permutation Eu hard rand perm distinguish 7 Distinguisher Byte Substitution: $S(x) = x^{-1} \cdot C_1 + C_2$ affine cipher over GF(28) · B · 0 × 03 00000010 000000011 • x+1 = x2+x = 00000 110 X A B C D

OS 10 11 06

U

Mix Cols

U

V

V

V

Z 10 = 10000 11 = 10001 05 = 101 06 = 0110 w = 2 · A + 3 · B + 1 · C + 1 · D = $(x)(x^2+1) + (x+1)(x^4) + (x^4+1) + (x^2+x)$ $=(x^3+x)+(x^5+x^4)+(x^4+1)+(x^2+x)$ $= x^{5} + x^{3} + x^{2} + 1$ = 00 101101 = 2D