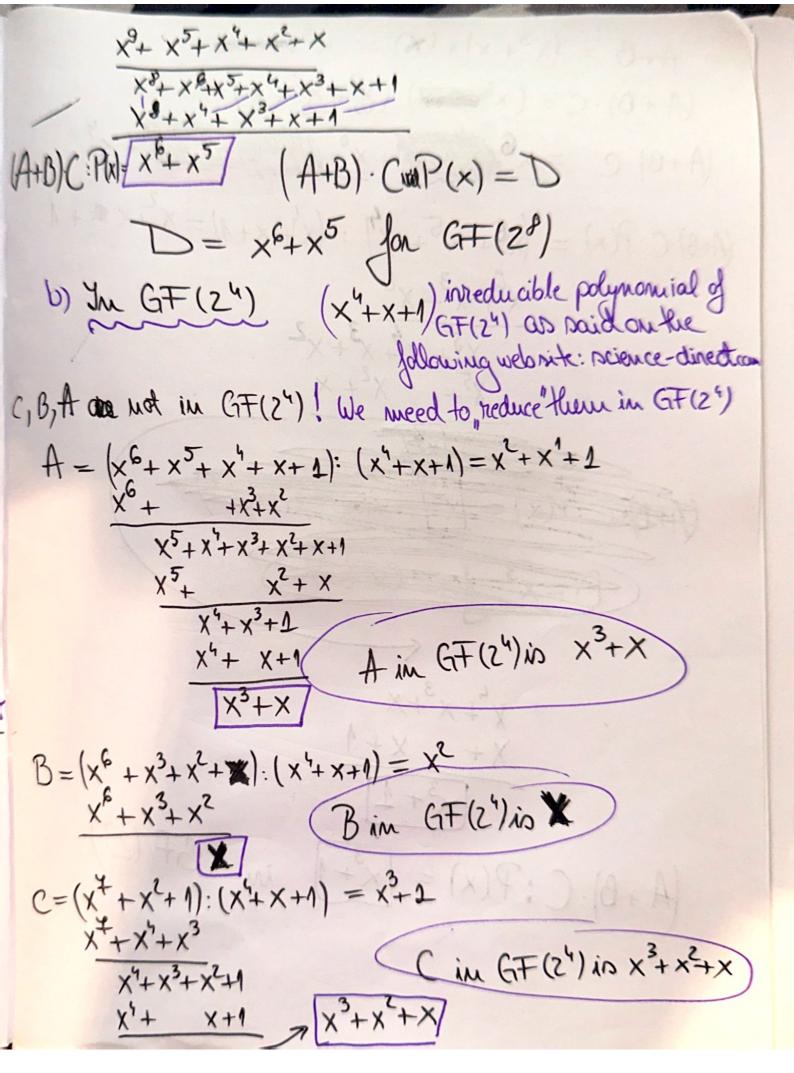
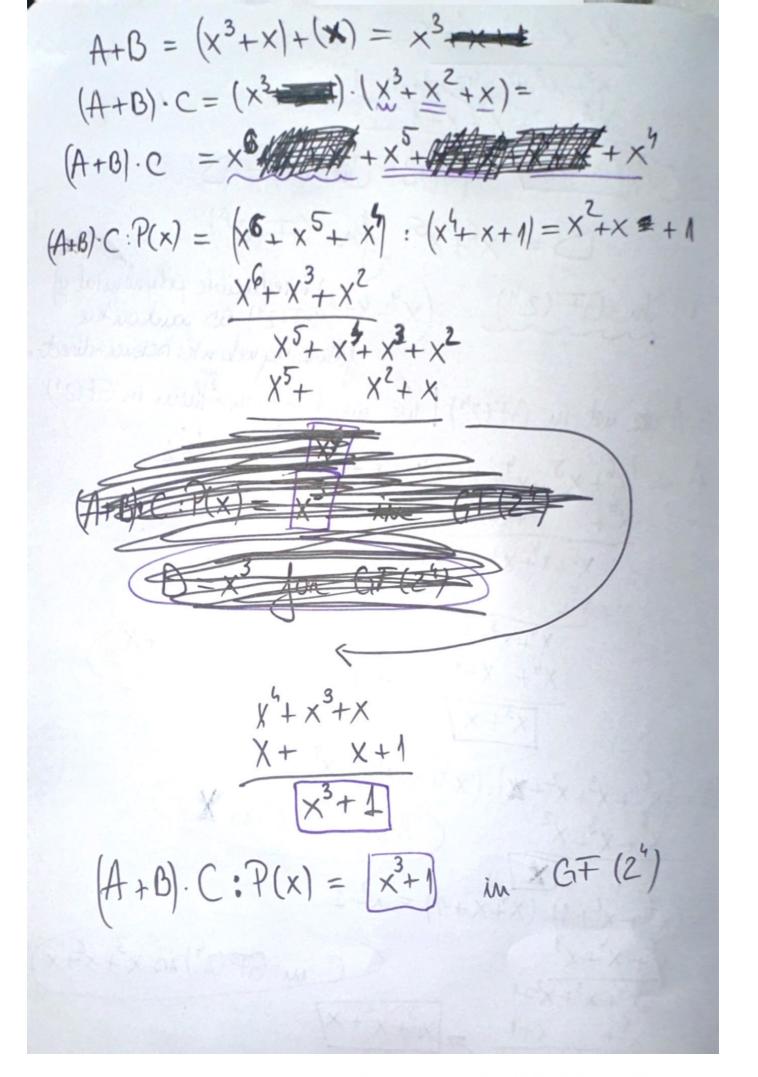
Seminar 3 Exercise 1 (Rijudael Block Cipher Algorithm) A= +3,6 B= 4E16 C= 856 D = (A+B) · C = ? (in GF(24) & GF(29)  $A_2 = 01110011$   $B_2 = 1001110$   $C_2 = 10000101$   $x^{2} + x^{3} + x^{4} + x + 1$   $x^{6} + x^{3} + x^{4} + x^{1}$   $x^{4} + x^{2} + 1$ a) In GF(28) ({ x8+x4+x3+x+19 m) polinomial of GF(2)  $A = x^6 + x^5 + x^4 + x + 1$   $B = x^6 + x^3 + x^2 + x$ Jon each %2?  $(4+B)=(1+1)x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+(1+1)x+1$  $(A+B) = x^5 + x^4 + x^3 + x^2 + 1$ C = x+x2+1 + x5+x4+x2+x5+x4+x3+x2+1 = (A+B)·C= x12+x11+x10+x9+(1+1)xx++x6+(1+1)x5+(1+1)x+x+(1+1)x+ (x12+x11+x10+x2+x3+1): (x8+x1+x3+x+1) = x1+x3+x2+x+1 xr+ +x1x+x+x x"+x"+x"+x"+x"+x"+x"+x"+x"+x"+x"+1 x + x + x + x + x + x 3 X10+X1+X8+X5+1 X10+ +X+X5+X3+X2 x3+x1+x1+x3+x2+1

Scanned with CamScanner



Scanned with CamScanner



## Scanned with CamScanner