#flo #disorganized

---

1 | **let's go!!**

Alice and Bob wanted to exchange information secretly. The two of them agreed to use the Diffie-Hellman key exchange algorithm, using p = 13 and g = 5. They both chose numbers secretly where Alice chose 7 and Bob chose 3. Then, Alice sent Bob some encoded text (with both letters and digits) using the generated key as the shift amount for a Caesar cipher over the alphabet and the decimal digits. Can you figure out the contents of the message?

H98A9W$_{H6UM8W6A9D6C5ZCI9C8IJBACIFAI}$

picoCTF{M43F4B$_{M1ZR3B1F4I1H0EHN4H3NOGFHNKFN}$} h98a9w$_{h6um8w6a9d6c5zci9c8ijbacifai}$

picoCTF{C43V4R$_{C1PH3R1V4Y1X0UXD4X3DEWVXDAVD}$} ?????

0.000228317094759−0.000156369801965i −0.003388682514055−0.002559342592582i −0.020711023763668+0.0617869
1

0.026936273599087

−0.156975118120879

{{0.000228317094759+0.000156369801965i,0.000228317094759−0.000156369801965i,0.000019543959048,−0.0038680

−4.877111838242915+14.549833022334499i 0 0 0

0 −4.877111838242915−14.549833022334499i 0 0

0 0 37.124660035896274 0

0 0 0 −6.370436359410444

□ □ A

{{0.000228317094759+0.000156369801965i,0.000228317094759−0.000156369801965i,0.000019543959048,−0.0038680

Power[(123){{0.000228317094759+0.000156369801965i,0.000228317094759−0.000156369801965i,0.000019543959048
1](41),n]{{1},{2},{3},{4}}

{{a},{b},{c},{d}}=Power[(40){{0.000228317094759+0.000156369801965i,0.000228317094759−0.000156369801965i,0.0000
1](41),n]{{1},{2},{3},{4}}

1/(2.6686294803 + 1.2425111682 i)^n + 2 / (0.10947922194 + 0.46692803193 i)^n + 3 * (-0.0032069238734 + 0.0025772731889 i)^n + 4 * (0.0046428436925 - 0.00077193357037 i)^n (x y z a) = { {1} {(2.6686294803 + 1.2425111682 i)^n, (0.10947922194 + 0.46692803193 i)^n, (-0.0032069238734 + 0.0025772731889 i)^n, (0.0046428436925 - 0.00077193357037 i)^n}, {2} {(44.560914245 + 7.408835600 i)^n, (-2.6626956746 - 6.8609841000 i)^n, (-0.11905595856 - 0.09568039096 i)^n, (-0.029576940269 - 0.0049175536838 i)^n}, {3} {(893.14976758 - 0.×10^{-11} i)^n, (177.19838239 + 0.×10^{-11} i)^n, 9.6002938737^n, (0.59537961435 - 3.7383980371×10^{-40} i)^n}, {4} {(1184.6407165 - 3534.1253570 i)^n, (17.160437605 + 51.194540956 i)^n, (-28.232186511)^n, (-0.17699846062 - 6.8522749741×10^{-40} i)^n} }