Allages ston kwdika

1o

1. Vgalame to encrypt 128 key expand branch epeidi den xreiazetai

2o

1. Valame sto in kai out pinakes 32 thesewn gia na miazei me to 3o.
2. Kai ta kleidia kathws to plain text exoun ton idio megethos sto 2o kai 3o kai einai 32.
3. Valame to kleidi kai to plain text sto testbench, kai to vgalame apo to main arxeio.
4. Vgalame ta temp
5. Vgalame ta nr kai ta nk apo to testbench, kai ta isagame sto main, gia na miasei me to 3o
6. Ksefortothikame ta nr kai ta nk(0)
7. 16 bit to in, key, out
8. Epese sta 1862 otan valame mono state kai key. Vgalame to in kai out.
9. Ola word anti gia char gin a miazei me to 1o

3o.

1. Vgalame tin aes\_main gt den xreiazetai sto arxeio(0)
2. Tha prospathisoyme na vgaloyme to type
3. To vgalame apo tin main
4. Tha prospathisoyme na vgaloume to out
5. Vgalame to out kai afisame mono to key kai to state
6. Tha prospathisoume na vgaloume to type apo pantoy
7. To vgalame apo ola kai exoume 1059 latency
8. Vgalame to const in out\_enc\_statemt pou den xreiazetai
9. Vgalame ta peritta cases gia nb=6 kai nb=8 opws to nb apo to InvershiftRow kai byteSub
10. Metonomasame to statemt se state
11. Valame tin Rcon0 stin keyschedule alla den allakse tpt
12. Prospathoume na kanoume ola word gia na miazoun me to 1o
13. Kai ta kaname
14. Vgalame to worda apo global kai to valame mesa stis stinartiseis (kamia allagi)