Сини Владисив ККСО-01-20 КМЗИ лаб. 4 в-21
Предитить вариант криптоградической ехения, отвениящей спедующим треовваниями.
Ангориты инфрования с мобым типом защетия виоков и проверкой ценостности сообщения, с выршостную помиять.
Тишно ОТ 2211 бантов

Параметри криттоградических пришитивов:

SCTYPT: Степень парашеньности p=1, размер внока r=32, слотеность N=40.96Согласно откритичи источникам минимальные требования по помнеми для scrypt 128. N. r байт B данном случае 128.40.96.32 байт =16 можит 0МАС: для вырыботки подмночей используется рекомендуемая NIST для имограв c $128-битичний биокамий константа <math>0 \times 8.7$

Протокой сообщения:

gumen comi l'onte uniquamizappouqui zaum probamos Tor mobersur coosagenae Tor mobersur venocomiocomi l'osaim + 16 saim 17+1 2224 osaim 2241+1 16 saim + 17 mo nogaimes na bxog exerce zaumeppelarius:

conte nocregobamentriocome soliim mouzbaterioù grumer sur el 256, uniquamizappouqui bermon IV - nocregobamentriocome soliim quintoù 16, riaparionax oppazoi, grumen 16, riaparionax oppazoi, coosagenue no brukonucarenquy mamon unique brigaim coosagenue no brukonucarenquy momokody

вишеописанному пропокому и пороменая фраза
Возмонения три исходог работи скеши денифрования

- genneppobarrece coordigerne

- coodingerme o omnober noberma MAC

- сообщение о опшоже в протоконе приначного сообщения (в случах, если дмина сообщения воные им меньше 2257 + L)

Com Bringmand KKCO-01-20 KM3U 100-4 6-21 Скена зантеррования: plaintext (2211 Louin) passuard salt SCMAPE pad with 13 random* bytes (16 faim) key 1 (32 daiima) padded text (2224 Documon) GOST 34.12-2015 - CBC encryption 6057 34.12-2015 - OMACI digest key2(32 daima) OMAC tag (16 Sacim) encrypted text GOST 34.12-2015 encryption (2224 courna) tag (16 davim) un, ognaro nociegami daian main guma naggima Tlak
kara gamaar exemo npegnomenca quicomobamenti pazule OT, mo spegnaraemor re brucorbame e korien pazule norgamena, a cyename oce samme engrantimu *B ISO 10126 ucnous yemen nagguer engreuremen danima-

