קריפטו:

גודל מפתח ב Salsa20: נבחר ב 16 בתים. (שזה 16\*8= 128ביטים).

נבחר key = 103181c805e46f17ba2946318178a14451d

nonce =

מתוך כך אנו נצפין ב el-gamal את המפתח (של Salsa20 <16 בתים>), מכיוון שכל בלוק בsalsa20 הוא בגודל של 64 בתים אזי נבחר בP להיות מספר בגודל לפחות 16 בתים על מנת שלא 'יאבד' חלק מהמפתח שאנו מצפינים,   
לכן נבחר:

p = f0f0f0f0f0f0f0f0f0f0f0f0f0f0f0f0f0f1

אשר גודלו – 144 ביטים = 18 בתים.

נבחר ביוצר:

g =

כאשר מתקיים : ואכן מתקיים כי P הוא ראשוני ולכן הינו זר לכל מספר מלבד 1 וP עצמו.

נבחר בd בעזרת פונקציית random אשר תחזיר מספר בין 2 לp-1.

d =

בנוסף, בוב בוחר במספר K באופן רנדומלי – גם כאן נבחר בk בעזרת פונקציית random :

K =

בנוסף, נבצע חתימה דיגיטלית בעזרת RSA:

מפתח פרטי בגודל 1024 ביטים:

private\_key = 0x165ecc9b4689fc6ceb9c3658977686f8083fc2e5ed75644bb8540766a9a2884d1d82edac9bb5d312353e63e4ee68b913f264589f98833459a7a547e0b2900a33e71023c4dedb42875b2dfdf412881199a990dfb77c097ce71b9c8b8811480f1637b85900137231ab47a7e0cbecc0b011c2c341b6de2b2e9c24d455ccd1fc0c21

n בגודלו 1024 ביטים:

n = 0xf51518d30754430e4b89f828fd4f1a8e8f44dd10e0635c0e93b7c01802729a37e1dfc8848d7fbbdf2599830268d544c1ecab4f2b19b6164a4ac29c8b1a4ec6930047397d0bb93aa77ed0c2f5d5c90ff3d458755b2367b46cc5c0d83f8f8673ec85b0575b9d1cea2c35a0b881a6d007d95c1cc94892bec61c2e9ed1599c1e605f

מפתח פומבי בגודל 20 ביטים:

public\_key = 0x10001

מספר ראשוני בגודל 521 ביטים:

1ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

ובעשרוני: 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151