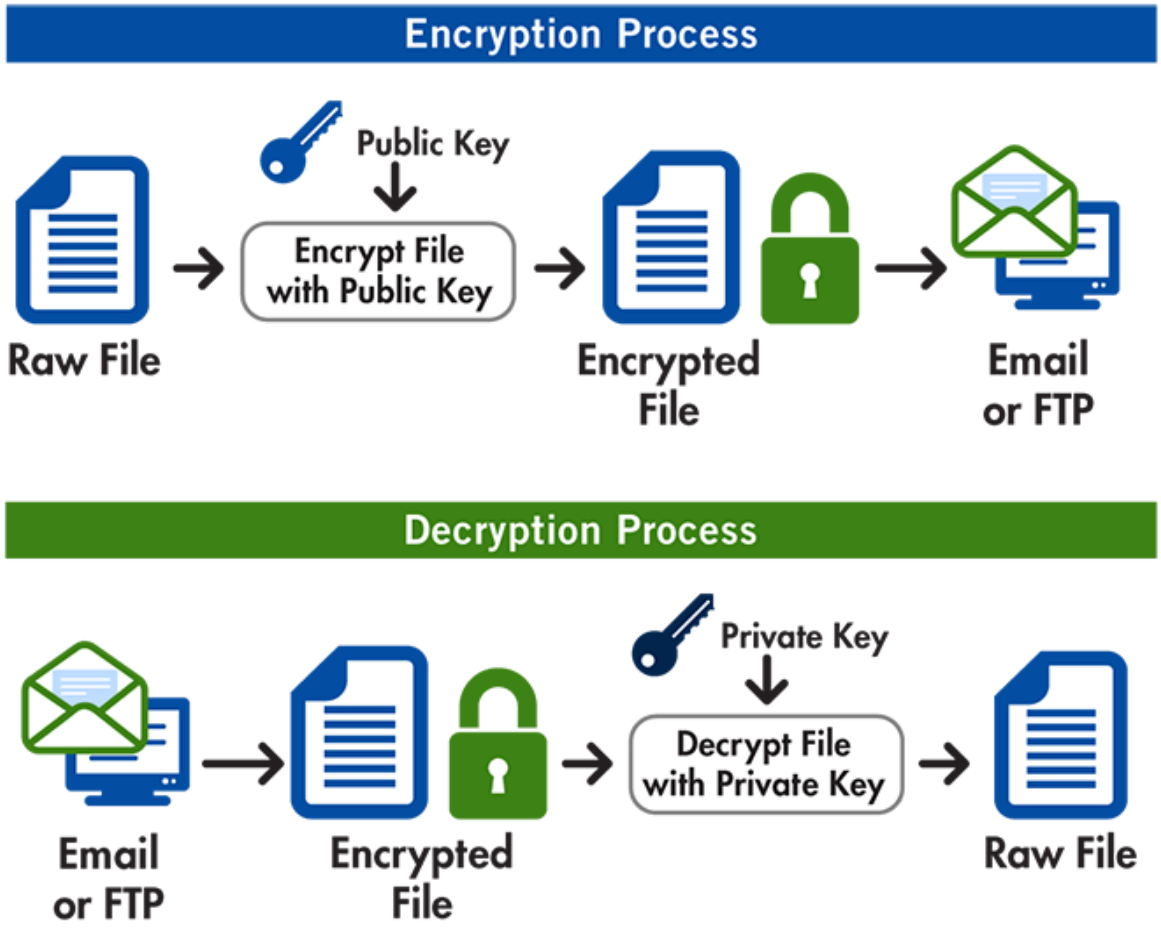
Basic Principles in Networking
Assignment 6 - Pretty Good Privacy
Pair 29:
Nguyen Xuan Binh 887799
Nhut Cao 906939

Section 1: Goals of the experiment

Pretty Good Privacy (PGP) is a security program used to decrypt and encrypt email and authenticate email messages through digital signatures and file encryption.

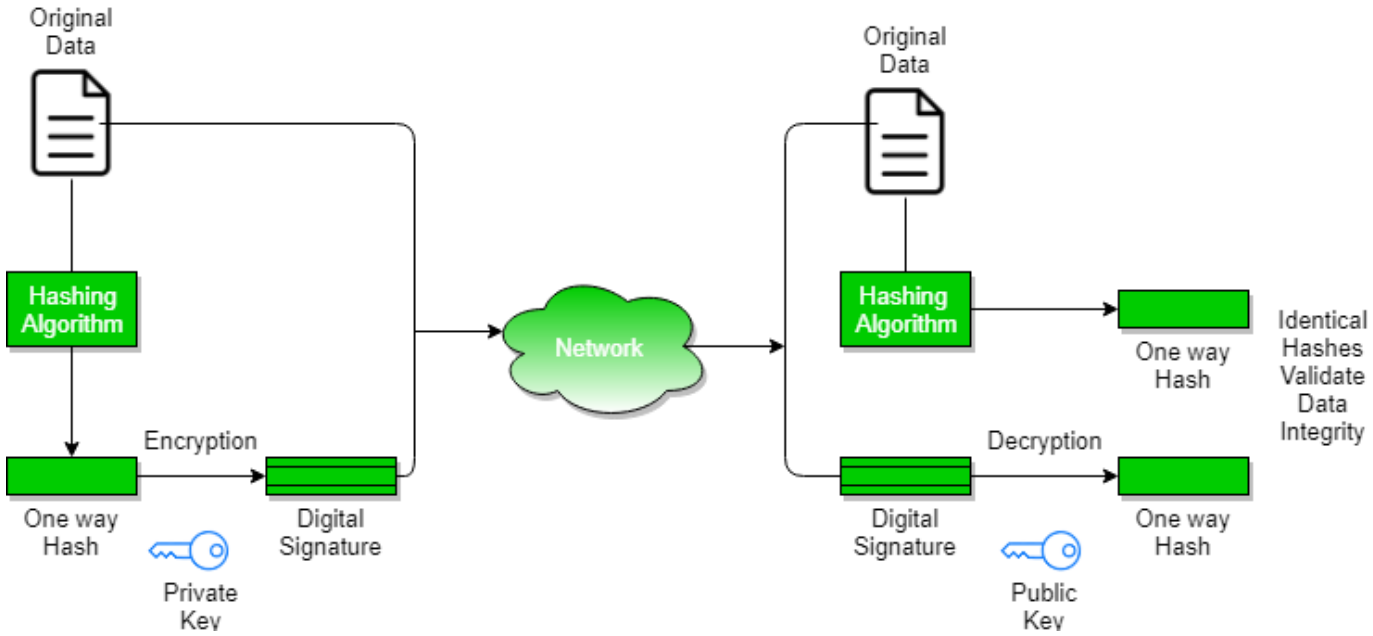
Email is a prime attack method for cyber criminals who can easily forge messages using a victim's name or identity. PGP aims to solve this and enhance email security by encrypting the data and adding digital signatures to make the communication method more private. PGP uses asymmetric encryption that utilizes two keys: public key and private key. In this report, a simple plaintext and attachment encryption and decryption between two users on gmail are implemented. This report also includes digital signatures and verification.

1. The encryption and decryption process of PGP are illustrated in the diagram below



The user thus sends his public key (to encrypt the message) to the outside world and keeps his private key (to decrypt the message) only to himself. Other senders can encrypt sensitive messages that they want to send to the user by the user's public key. Once the user receives an encrypted message, he uses his private key to decrypt it.

2. The digital signature and verification process of PGP are illustrated in the diagram below



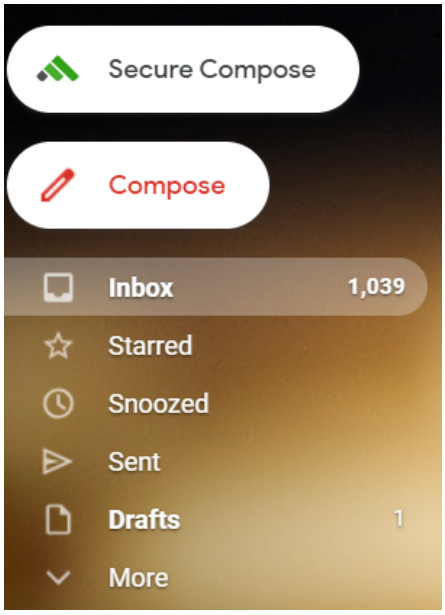
The sender first digests his message through a hashing algorithm and then encrypts it with his private key, turning it into a digital signature. He can also encrypt his original data. After that, the sender sends both the encrypted message and the digital signature to the recipient. At the receiving side, the receiver decrypts the original data as illustrated above, and digests it through the same hash algorithm and obtains hash-1. For the received digital signature, the receiver uses the public key of the sender to decrypt, which returns hash-2. If hash-1 equals hash-2, then the receiver is sure that the message is authentic (actually coming from the sender and not tampered with). This is called digital signature verification.

Section 2: Experimental Setup (Details of the experimental setup step by step)

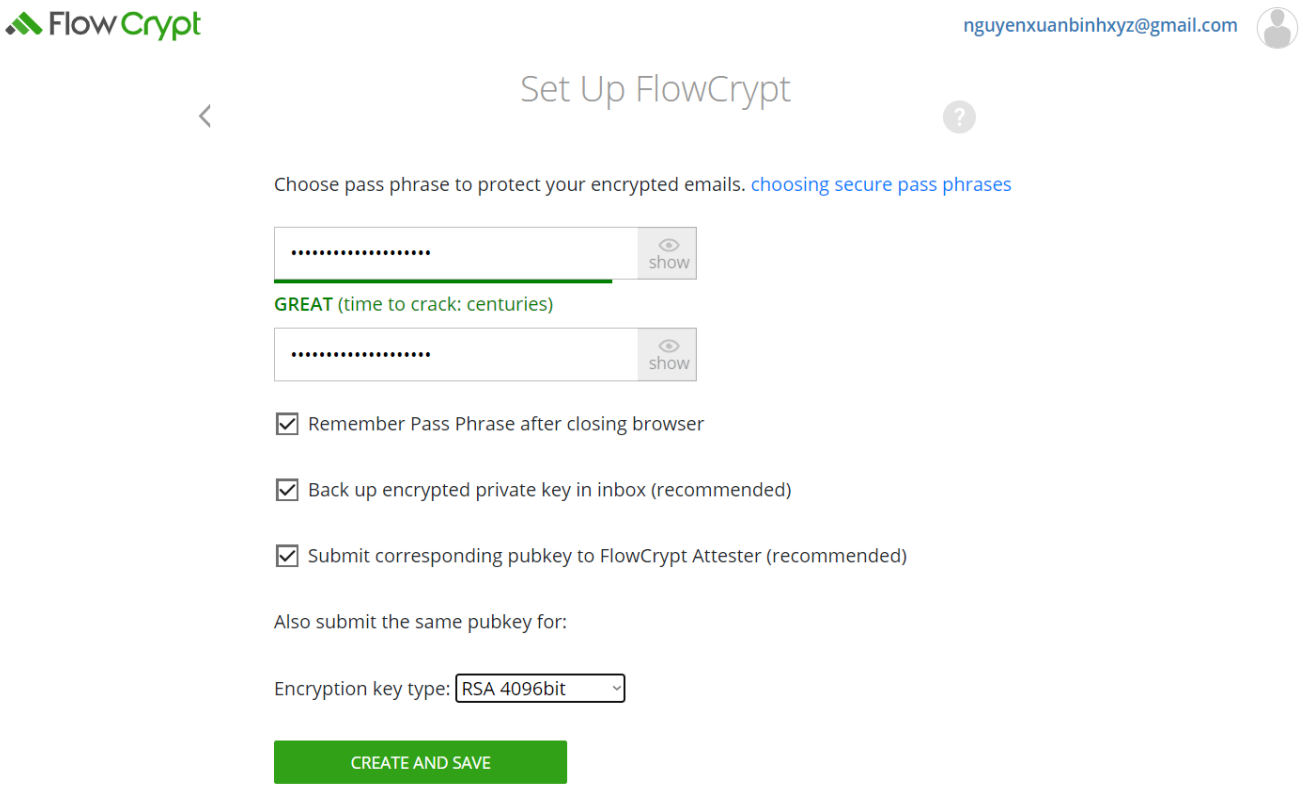
There are several software tools that implement the OpenPGP standard such as Kleopatra (GPG4Win) and Secure Compose. In this report, we install the extension software called FlowCrypt, which can both implement encryption and digital signatures.

The software is available at https://flowcrypt.com

After installation, the extension is added to the browser and the gmail website has an additional button called "Secure Compose"



Now we open the extension and registers the key pair for two accounts: nguyenxuanbinhxyz@gmail.com (Spring Nuance) and xuanbinh.dev@gmail.com (Nguyen Xuan Binh)



After registration, each email account has two key pairs and they are now capable of sending and receiving secure messages from each other

- The public key of xuanbinh.dev@gmail.com (Nguyen Xuan Binh)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

xsFNBGI8pKQBEACealisKguxQiMD5LHGqC5YdnMRH/FyZu/n8QsJAWA1Jxsf
Q5ds3wvx+BjSRApF2g9QPXtQNq1oRFOPFutrIrHSDp6DRR26zT6n/sG0VcoU
iMH35kRQp+I3urD3nea8LAIiqITwQSjEFYsF2rxoMP/83wzIWapgwwDxQNqO
pPf3h/5S+IQIpCnNP1oPbLK5fsWoRdC2Xo4KSKxyKzZA9TaukQXiE8qitiAy
zPGQs0kTR/QVnCwdyoKQwHDj+CTdjOBscu7i1ukaCeIAibbWoR88E+2C6BD9
yJPq8xJow/abVLyIltYFIEiRcBdaCEYjJVoRGgcUdCjU23zYPOvc/SmprSM9
lsOtQJkP/PuMMUagoZ6/brlzPQMOu1F+BKJdkI0M/JDcnvp4kSRI0dvTXQHM
KFDL0ZLFwSIfbM+Cufmw8MUz/uaQjRaFJxyRuzN6sHI9unhv3MF0l6vpPEgk
1YWiCGJhkSdcXsKvpP8g1oWTdZcvwQukATr7SHbWQrSfYB1qZlA/ErxItJ/S
8g3fQSxVSiFD9MbtVYt43KWTv3zBIMcBbigbrIFOGBMj2edauc15UDMibSWV
p2KmqiZdG+BIUCiHFixgKJbaPW8hYYGCdno9Zeqh8tP56ugC8Ai4oYwfjAJy
DYCem3dYkeTnqPO1HVuZTtmhaFEnTKa78gS4XQARAQABzSlOZ3V5ZW4gWHVh
biBCaW5oIDx4dWFuYmluaC5kZXZAZ21haWwuY29tPsLBjQQQAQgAIAUCYjyk
pAYLCQcIAwIEFQgKAgQWAgEAAhkBAhsDAh4BACEJEJp9h8ZGx3nvFiEEwHBV
kiNFpmYt41BLmn2HxkbHee/qUQ//XRvTRjuG9bjtA5sULrE+KkHUi2w2CGeA
HEegLyMmDg7rCuMoGHNueafQlt5/4vqr/sd16/uGIuqDNsKL+G4aOWKjbRzS
hl0Wokl7xOni0dwDqKUgrdbTN57PDw5bE99is9iva5m7xhP4xezxNDqkmCZv
PeMF+Oke+pf+4Iq1CS+ihXm0ky53lE7BQSiwCK2V/YDUYqFlBU9a6URybgeM
gcJEDHu2udDAYc6gGN508SnfLukvYqdcz54l5V064O1Xbhf3UgI9FM2+dm39
DmKt0C+HGWBP9nTh21vliYLHAplaof+YOUo4rcBbt2tbKPQ18Jr57T/ZE0qP
XvLJwcF6U1p4eSf9p5pZyBYzIv3ukBRDRorDYZwPtHWWNeIRvBOnmKXqoBE+
gO0vDx2MFwG1ynWY05jvI9U5IuKP1WnxxHKzlTpE7IglaS/9xESLrXsXMXks
y6ihmp+S40eZO4J5z9stOGL4S6Pj3kgsdcmS2jNta6rAlrkts9K7BIy6zTLw
4w7S8DleKg3NRr1BUgNLWtczoTxd82zGy314CDGQVaMni6lRsIDBabDcvyKm
fJS7KWsjG1m1kD49ei9ErcjIIKQMJFLN+JZ3DXaaFWkld5IAmAa6nhuSF246
zVb4Lui1oN00BkMgg7SWh+fC24Zn4tg+WOKD8/dignIsx+cYoAPOwU0EYjyk
pAEQAL5NLbBD/3fbq2FjfNRXgcxQ67l4s+kVTyZ9G8YddFuLPExUZ4HRS+4v
nn+SCQe2AC+D6fPDweU+vf/nDPg8mDgxqfoXQmsoxy1iumdcT4nn5Nm63T1l
ZTzz0jgs9BMgVeKFaFRWm965tpEDrm0EIm+CflWxYTd8RSy0G6C8L4V5NyUj
t1TPC33sYqXRVDG9a8DtLUofcTsHhho79qX9JBn170xKN2UIUaMMFljJKv4h
8uaQb4BEgI236EwqrlHYuzWrd7KAhaU8U/yA4/Z9XPM3h47S7j0dm3jCMLTQ
sO+WnC8SeWAeeHcGDgLSdIGncQHKLwlDfsrMAk5fApQF5LRW9V5IMcEIfmIM
+zuv4+ZwyPeEZWewQmBHx7UH9CxtyMM0WMzn1Q+9KzZiSr0ONlpCfh4V4Yem
uuUCpOWMywkyr/m0/bB/MQ8tD0rFWCOwY9yMMNIRplTDeoGrjily1nZqu/EE
wNlrruuMgJAtnRjJsNotkB/iy1yDlZ37VEJ1Z3+cKTKPGsvfwZEBFnnZQ6cC
/uazWFs1QzHKDQS96iWc0F9gJF9EtiY4zpj6Y3Yd45kAkILlkTjiy/DQBIwG
dHvaV7OfsvfafLe16Z0RqFqspANlOmjwXVeZritHo/myJ5hcwUWbxKaL3CHX
cPH4ZB2eh3Ax53zfxxRj5fUeweD9ABEBAAHCwXYEGAEIAAkFAmI8pKQCGwwA
IQkQmn2HxkbHee8WIQTAcFWSI0WmZi3jUEuafYfGRsd57yFyD/9MtVHe0hCb
xSR6rILfpbOyosoQIFBFNvwe4ytIeWnKBXB68iyQ75qs/5f1SRndr+jDEdrt
7ygTXtLelAhm9NI3YqZzOQaF/NAKmgz0jqBF9yV3fzTcMlqclgCQDK6UhckY
Bq0BeogffBqPA345KZFzetbd7hberv3hK2CNoyLS8VAoJcVtd3G/VKzoAft+
W52L+kRydFMe8aN0xJuZGG2D9LMPR4ab6hm9XF//yLcqxHQilH67ZR5oNVEn

g24xSKngBuWr18LUIreNCt+NaHUo8wMFE3CPiEcF511Dm2B80A3LqhjZkZY0
H17Kjbonw6xc7JrvpPo0nIufGxPcJqOdBbDh5YI3vx7HKA41aFdyih4pQmzn
zXIUmefDzJFIpWaqxntHJ801bGHBHotLyBes4Tp0G9DcsDULW3hFXoDtsdjY
Mfu+bbZ12wmFszqOaDEgs/KzDvlYaJBBaiYI08cqCRm68h3ZEvbxUxl4emPa
lRiwh1xOn0MXHAa7M0BYqAy7eetlBY3tiLIe0cH2oOy9tUbheVYv1/1gNkbC
Jmma99ZJS78ccRI96/rdWvH7+DfNqvn/jFNf+L9Jdwrx43U7musnYG7LQoOT
/2oFAtbs+YpawOH41P4st8OCe2BRh8XGJP2yQry8H3VAhXUYXpZZ7W9/a+up
8SScfQ7+/ArQ/w==
=KyTz
-----END PGP PUBLIC KEY BLOCK-----

- The public key of nguyenxuanbinhxyz@gmail.com (Spring Nuance)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

xsFNBGI8pRIBEACe7PgMeRSubg9O3sMd7dvk8brJH7ZzfL7mrno9CqEpGxCs
iGM8bJv8KkKQQd4WO4Pi+9bDioKQnHywfIDweb+Pxz6MIft68LHkmdngIQ4R
0mD+ibmTMBmv4Ug5ZBe9qs8KdV/d9uftN876xWd6hAqXhRd/8uKJ5B32Jvde
RRtLTe7GD2/VLyedORp2VJRpkoIuZzuaNtvhDbSIbDlj/ASucU3GRUdxE0RX
9bUCU5lZTcUPyQQXIu8U0dG7/KaRCsyKuZNBi8ZKJ6MciEs1HwxXQo5QCz9y
K0XSd6Suo5CEcweDjaslh/vhuW7EP2KGqRpwi8WlibsOe48or/1mBy3jjd6f
6CMg6ay03NyOpTdcRmebyAg0ncT9zav7C3wMt1pQ2Lt/rpmb7HgbnbTjbaPj
KMElb+fYM+ZgzgMyFrzDlwcUxqan6uIeYhHkxlRsulGoA6As47b/iGtglH82
BNOxkEytr7d0Q7axoa5ZNUhXdKDYEsWTrP8oF+7Ozv1w6bkK1UFNHs/RXV9b
jrd0C2QqqdsjvbOu0HSOU0uF9I2cPj5QLliDxTgnFUKx1u6TY+RKiY/h3WwX
kk1fxuUL9uon7xF2wOsDiLAqb0275FON+J+FxY16enc0tSjOrTO5H7ZdU1l4
0ksi3wEQ+wshwfg/q7cWqZhYiO3u3pi4NWNkjwARAQABzStTcHJpbmcgTnVh
bmNlIDxuZ3V5ZW54dWFuYmluaHh5ekBnbWFpbC5jb20+wsGNBBABCAAgBQJi
PKUSBgsJBwgDAgQVCAoCBBYCAQACGQECGwMCHgEAIQkQHgUe/f6Et1kWIQQW
YLNFC2yeE9sI60ceBR79/oS3WVPeD/9w0pYPaSQwteOm57tjhZXXfbHMxGXH
xEiClP/XNuIovcP4I8rN4ENK0zzi5A0IAkxhX/yszYugt8M1Ke1muDmTk6dM
u8H7mWLKtqCKKRzui/cTwgQ8rzVDnvfA1dJtD5Tu8dVeBmv8KHC6qyD+EIpG
RI57pYgymB+Kq9Xdfc1ky0MFnxqcAaHLlcqjqP+00+kg1/w6HMv7+M9vYoxS
IYqFbPhRdGhqWvtbDN8MzLm7b7S7IZWRe9vJ0iTq1ggulOzEgYrr/NOni+z/
2p/O6D8NhD6E4VTBsicuHE60sp8+JK2YA+GdzbjNWYO6xwT1sIUs9fRGLBEA
H1OQ/9d7mOkDhOWKhZvzBWYlucM4PX0luLI3h2PvdOmzyOntmtaDGhr1skYz
WEcAU6huLdPYOts6jKIVFosRvYqPEMLkm1wHS2fpde5LZAhhb8E6hjQU9RLH
MpiNcfXCvaBPziJ8VrPIC18gtx6fK3jjxWAbwmF++E6U0OAt6Z3e4sEjiCpB
fhl21/CDZ9w734S8pz7OxlGmqYEFH64vofrzgpzLA4CB4QhZGZ+czUNmGf0p
9tSJrSk3Xon5fmJl3QIDEN1DIU9J2yrbdQV3Rd2gALstVgu5tRArJXhQ/G1G
bmrbuWryvTVIXKycuUfA+FPjvxQ94hjRvWkg4xSVV/pyhV2vVL6UFc7BTQRi

PKUSARAA0iSda4Zw9u5Ew/Z5jrRRlZAbJHXH1dTR1sLYc8JVgkXZx28Q5NeS
Z7Am+Xo5rQqvjwVcpgbRwBfY9E35GIBtD0NKnSvmMA6ELXwW2LATHfMSumfo
Ia7qiJCGut+rzi13pSmWp38NfUqY1rd4xjWWPo+Dz3Jyjcf062HzzeREVe40
xy2QNT/pJetCns64S5psQKEVPmOQK3eImRWOtSryuw/5ew8UC1dUBOW5juAC
LgBw2eukTbhGCAaOJ3fyWTcu2RxOVZJQvLdGkcJ2pXR5k2tGnQQPcNAO6tOq
CT9Rzb4ekS3YpCxLzP8cO86LHP9e+/jIPJkdMDX+IzqG2Bvs3z1OYtrCoVSi
+u84XWEhHyAdj56MutDltIeQyML3Wlx8YzM5C0emjF2KcoSvgRi3pE70evKB
1x8uEGpuiFZgNDtCLyLlsQvbqNFtjnMQNTTW4Sa9fNglU1Vprd3OF82RJXp5
pH2JO/E5jvUNY4Fy5ZQz9PreefOdBtWXlBZcEIEgwcIsHoTqRW8WHLzSJZGq
4BNtNzBsitTZP77aqV4JkU1ytyX+Rv6YyChpQZ2x1JM5mb8cfcjnNpP/w8Ak
ZJ+h1S3pt95AtUnKjGbvKtyaErvSwP7oNYYwXcUtx2yoK7fnTKNsgi+IHCDl
/gCzlFVGsPf7UrPc+1JK8FG9fMs70/UAEQEAAcLBdgQYAQgACQUCYjylEgIb
DAAhCRAeBR79/oS3WRYhBBZgs0ULbJ4T2wjrRx4FHv3+hLdZevUP/3OIgIJd
SJS4EXVajwO/hm+Hp9baF6tQsb776LXDyMmx94WNDnOyX7vj/DCMnSHjQhXF
2w1u2Zt2jScaIGsCwm2sojm8NchsAwUaktX8SUVbRxjkdJUER6+Cj3Gz77/n
jE1FOQ2flsACsIdwG+5STcUXh9hyWlxcSlSH1ZbsZwQRcyFOL1IxadizxkLE
NoTAQYUX+23+3TC7f6fzKPHY4uobTcu1TQspBjx6ROyQAIK21zNSkE8HjV5T
OeuTipCT7yfsUjckING/SeGLYcHykPsYuvb6Tc7wPmwPy6rg20bf+ZxuNBa+
RbsDMDgRmBziunP5JNnqlymiSoDBVTQ3m0gt7a/ZDe5hxqdYZ2joBVxZgFQO
AF2P40AbaAPr2VlC6xnsgEoQT8DEXC41F6rPJ1qdw4WJBhAJCskXLvrDjNy0
77VmFt/MyEfxDS+J08u4nyZs9WP8qqldG30yk9J8aO3Yz92GlvAyMQ9W8sFR
sCqOensS6Yt3CXcmRItZqwfXupsIylOFPT24zPqA51GDQVWSFThid6T3K2JV
PcDqLdY9lJDjOfs5du825lgB5otAVnarlkfjkX+VXStLbR9xbx1CnIAifgQe
ZohSO8PcHY2XMAVdAuOT3BBqVfLfwSqQBSq0rK8XV9DOQr/JoRb8zy3Wdlu7
hwR5pT2Zhy7dKng/
=RSqG
-----END PGP PUBLIC KEY BLOCK-----

Naturally, the private keys of both the accounts are supposed to be private so they are not included in this report. However, they are still saved in the browser's data for end-to-end encryption and decryption between user messages.

For the next parts of plaintext and attachment encryption, they all use the RSA-4096 bit encryption algorithm. RSA algorithm is an asymmetric cryptography algorithm that works on a key pair Public Key and Private Key, as described above.

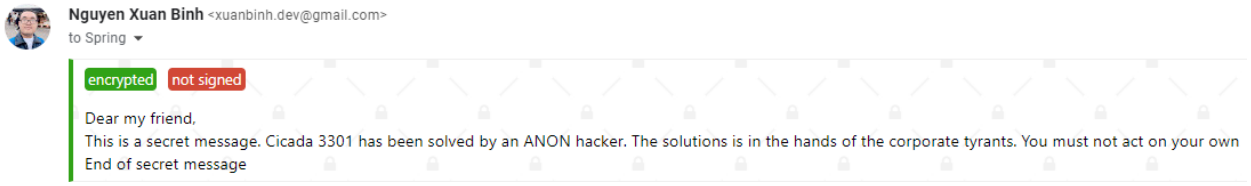
It is found that a 2048 bit key can be cracked in 100 hours, but it may still need to take many years to crack a single 4096 bit key. There is a law of diminishing returns with RSA key length, as simply adding 1 bit (going from 2048 bits to 2049 bits) does not double the effort to crack the key. In other words, each extra bit adds some security but a little bit less than what was gained with the previous added bit => 4096 bit version can secure the encryption better.

Some types of key such as the OpenPGP key pairs are desirable to keep for a very long time such as decades. Therefore, the trouble of replacing all the digital signatures may be quite high and it is necessary to have a long-term future-proof key length => 4096 bit version is preferred.

Section 3: Results & Conclusion

➢ Plaintext Encryption

Now we compose a short email from the account xuanbinh.dev@gmail.com (Nguyen Xuan Binh) to the account nguyenxuanbinhxyz@gmail.com (Spring Nuance)



The above plaintext is encrypted using nguyenxuanbinhxyz@gmail.com public key. Next to the profile picture, “to Spring” means that this encrypted message is sent from Nguyen Xuan Binh to Spring Nuance. The encrypted message of the above plaintext message is:

Nguyen Xuan Binh <xuanbinh.dev@gmail.com>
to Spring

-----BEGIN PGP MESSAGE-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

wcFMA6ryhkiVTS6WARAAr5is9lgmJccA+zCiGzor4rLiP5rO56aF43GXLLGY
GQpUYfQbjO3w9fkCUkWgIM6ORqX1k3u102zmjJCreUJWdAZAfTL+SPdpheOe
8XWV54vNHJZZv1Es0xjcwqVAmEUfabO5W0QtlqI0kZOiLtHorNA8/JGBBSpc
YcpDLB4d170LCrms4+oX/QCUECSuoMSIb2e5y/PUF1Fd8P2xoEOXhJaToakv
j1n1sav4ftTAq5ZEMey778nh7qqaZAn0pzDtDwU6V/fbGMYER5OzG9tigCUX
KyHgtHaqISguY/Ja1n0V8/9bW9biXfdKsiH/G+AuGNM9xrLwjDePaP/eqk75
uJq+tPQcsNTDuwJCDdKhNbKh8W0M+LU2RNY7jMOQSJ/ILL268fPWIVKAGZjh
Gb/bZ72G8Tjwt8Hm4lxYXBHVIU3DNKsN7vB/OarHkX7RXnIG4ocW236epiV3
L8h+OAoFHn/moar1xR/6KUDt2ynN1HyAoS6bX07BkzspFnq/4m6uXoq5ngJL
vLC000+I9EXqKbtiJ+0TxRVtMnHC0zoj9ICAB4k5NypgJC46LaDuVDXSyDNN
yXJL92ldnYBeUekI1GOSuWsfIGchPf42uwDYT6Gqe1BUjC1MhYYDUfhj2RNo
Jr7KgMF5JSd0Fmq95wlEUCxJbg9Z6hb1i8SGnyd+A9DBwUwDG3+Wt7MrCfMB
D/4vRf/omghHiTcedhlBg+JmkpaYrjctOVvHp84kALy0+wIOLIZdipQt8+Vj
NklM0m1LPH3YUJI90NYU44ZaGKwaZrFpDUn4FtH5AWm8JMOKXRTb7LGGj9R0
2eCXdvbBQ/xuFWiAoBopV9SO6b0u3+5wno8yBZQgOtxzDGxr0mx4QcqSFG0t
wM84DDyd0nJmj/oWaLNkEza1G8q5yI4CGXIBHVwd8cr+OuAPe1aYVJeKYuAG
BfWPzYKez1P5iH0APRUhymd7GYDv3FoJ3vwVfaFuAYqiSBUndNr1VDV2Z42d
XvER9A/ykPYWyrdoWmZ6f5TmclAvPyRppQeh9yEIGX09gCEmXvZg/5HfVBt9
exhcJ1R1FHhycjfs6QujpE6QmPsKHaNIaTwo4ouWjJOtZF5Iz+kSg+V8eLaU
fSLhsxHU2tzS0V9ZEZT05yaEBP45IspthB4ot5KymiTFLaqj1ZEHJzBVeAg9
cB1JzS1MTFnfAO8dliBMkW3otWX1+AUu0w8M71hk+YAEh93Ae26hy87DActZ
wmNKH8G7AoicmIB/GLgIKjYGbW8QICaNWZPUeEAkHJbCyqVfKpZajG0wELhw
GI5972ltbRSVOwVYjOqQlugWY9+WV1YfnwtAyIkt3M/sGRgyNIGzLwy36vbC
DoYIQZcUab/zhNyI2XnZZ5K/EdLAPgHJ5tcxLBYDW2PEoZ8WvpBjpd7g+Wvg
erRMnoldFyTrE+vVN8B84DqtVB77BUP41Ym/lj98dISHWShzhH/BvhsKrCst
ETGgg3s9Ok82bWasNonPXI74/Ovl4bR6G3UcK+0SQ1/4JB4Lr7B377SV4xmr
TNPV6dGYIJ2sBeliHav+NPg+PDJzguAURW2gv+c3Vn0VfSWy/BhE1pDuDdII
aRtL1BeuHPzeCXrtT37XgRvbEUSx6kV9rx/rPOpWyvqE8N8NVuKAvF5z46E5
lrCort/MVo+tbiqUz2KJBx/51PsTpfCJKFuHL5vLfEBYpHeInCXCYsKwvztm
2jwOeNol
=EN7R
-----END PGP MESSAGE-----

➢ **Plaintext Decryption**

Now we open the mailbox of the account nguyenxuanbinhxyz@gmail.com (Spring Nuance). Next to the profile picture, “to me” means that this encrypted message has been successfully received by Spring Nuance from Nguyen Xuan Binh.

Nguyen Xuan Binh

to me

-----BEGIN PGP MESSAGE-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

wcFMA6ryhkiVTS6WARAAr5is9lgmJccA+zCiGzor4rLiP5rO56aF43GXLLGY
GQpUYfQbjO3w9fkCUkWgIM6ORqX1k3u102zmjJCreUJWdAZAfTL+SPdpheOe
8XWV54vNHJZZv1Es0xjcwqVAmEUfabO5W0QtlqI0kZOiLtHorNA8/JGBBSpc
YcpDLB4d170LCrms4+oX/QCUECSuoMSIb2e5y/PUF1Fd8P2xoEOXhJaToakv
j1n1sav4ftTAq5ZEMey778nh7qqaZAn0pzDtDwU6V/fbGMYER5OzG9tigCUX
KyHgtHaqISguY/Ja1n0V8/9bW9biXfdKsiH/G+AuGNM9xrLwjDePaP/eqk75
uJq+tPQcsNTDuwJCDdKhNbKh8W0M+LU2RNY7jMOQSJ/ILL268fPWIVKAGZjh
Gb/bZ72G8Tjwt8Hm4IxYXBHVIU3DNKsN7vB/OarHkX7RXnIG4ocW236epiV3
L8h+OAoFHn/moar1xR/6KUDt2ynN1HyAoS6bX07BkzspFnq/4m6uXoq5ngJL
vLC000+I9EXqKbtiJ+0TxRVtMnHC0zoj9ICAB4k5NypgJC46LaDuVDXSyDNN
yXJL92ldnYBeUekI1GOSuWsfIGchPf42uwDYT6Gqe1BUjC1MhYYDUfhj2RNo
Jr7KgMF5JSd0Fmq95wIEUCxJbg9Z6hb1i8SGnyd+A9DBwUwDG3+Wt7MrCfMB
D/4vRf/omghHiTcedhIBg+JmkpaYrjctOVvHp84kALy0+wIOLIZdipQt8+Vj
NklM0m1LPH3YUJI90NYU44ZaGKwaZrFpDUn4FtH5AWm8JMOKXRTb7LGGj9R0
2eCXdvbBQ/xuFWiAoBopV9SO6b0u3+5wno8yBZQgOtxzDGxr0mx4QcqSFG0t
wM84DDyd0nJmj/oWaLNkEza1G8q5yI4CGXIBHVwd8cr+OuAPe1aYVJeKYuAG
BfWPzYKez1P5iH0APRUhymd7GYDv3FoJ3vwVfaFuAYqiSBUndNr1VDV2Z42d
XvER9A/ykPYWyrdoWmZ6f5TmclAvPyRppQeh9yEIGX09gCEmXvZg/5HfVBt9
exhcJ1R1FHhycjfs6QujpE6QmPsKHaNIaTwo4ouWjJOtZF5lz+kSg+V8eLaU
fSLhsxHU2tzS0V9ZEZT05yaEBP45lspthB4ot5KymiTFLaqj1ZEHJzBVeAg9
cB1JzS1MTFnfAO8dliBMkW3otWX1+AUu0w8M71hk+YAEh93Ae26hy87DActZ
wmNKH8G7AoicmIB/GLglKjYGbW8QICaNWZPUeEAkHJbCyqVfKpZajG0wELhw
GI5972ltbRSVOwVYjOqQlugWY9+WV1YfnwtAylkt3M/sGRgyNIGzLwy36vbC
DoYIQZcUab/zhNyI2XnZZ5K/EdLAPgHJ5tcxLBYDW2PEoZ8WvpBjpd7g+Wvg
erRMnoldFyTrE+vVN8B84DqtVB77BUP41Ym/lj98dISHWShzhH/BvhsKrCst
ETGgg3s9Ok82bWasNonPXI74/Ovl4bR6G3UcK+0SQ1/4JB4Lr7B377SV4xmr
TNPV6dGYIJ2sBeliHav+NPg+PDJzguAURW2gv+c3Vn0VfSWy/BhE1pDuDdII
aRtL1BeuHPzeCXrtT37XgRvbEUSx6kV9rx/rPOpWyvqE8N8NVuKAvF5z46E5
lrCort/MVo+tbiqUz2KJBx/51PsTpfCJKFuHL5vLfEBYpHeInCXCYsKwvztm
2jwOeNol
=EN7R
-----END PGP MESSAGE-----

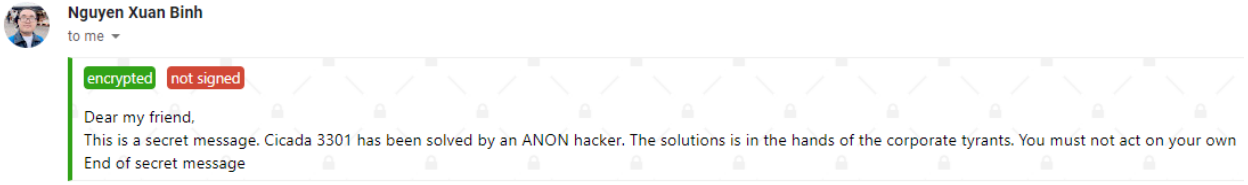
The above encrypted message is decrypted using nguyenxuanbinhxyz@gmail.com private key.

Nguyen Xuan Binh

to me

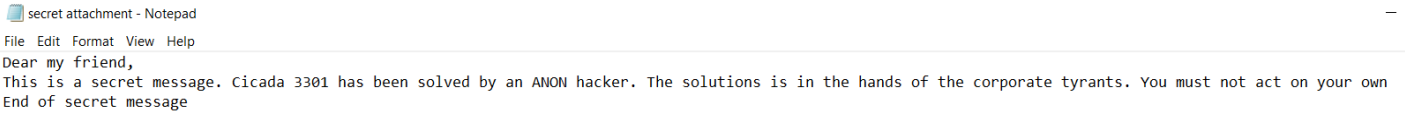
Decrypting...

Finally, the decrypted message of the above encrypted message is:

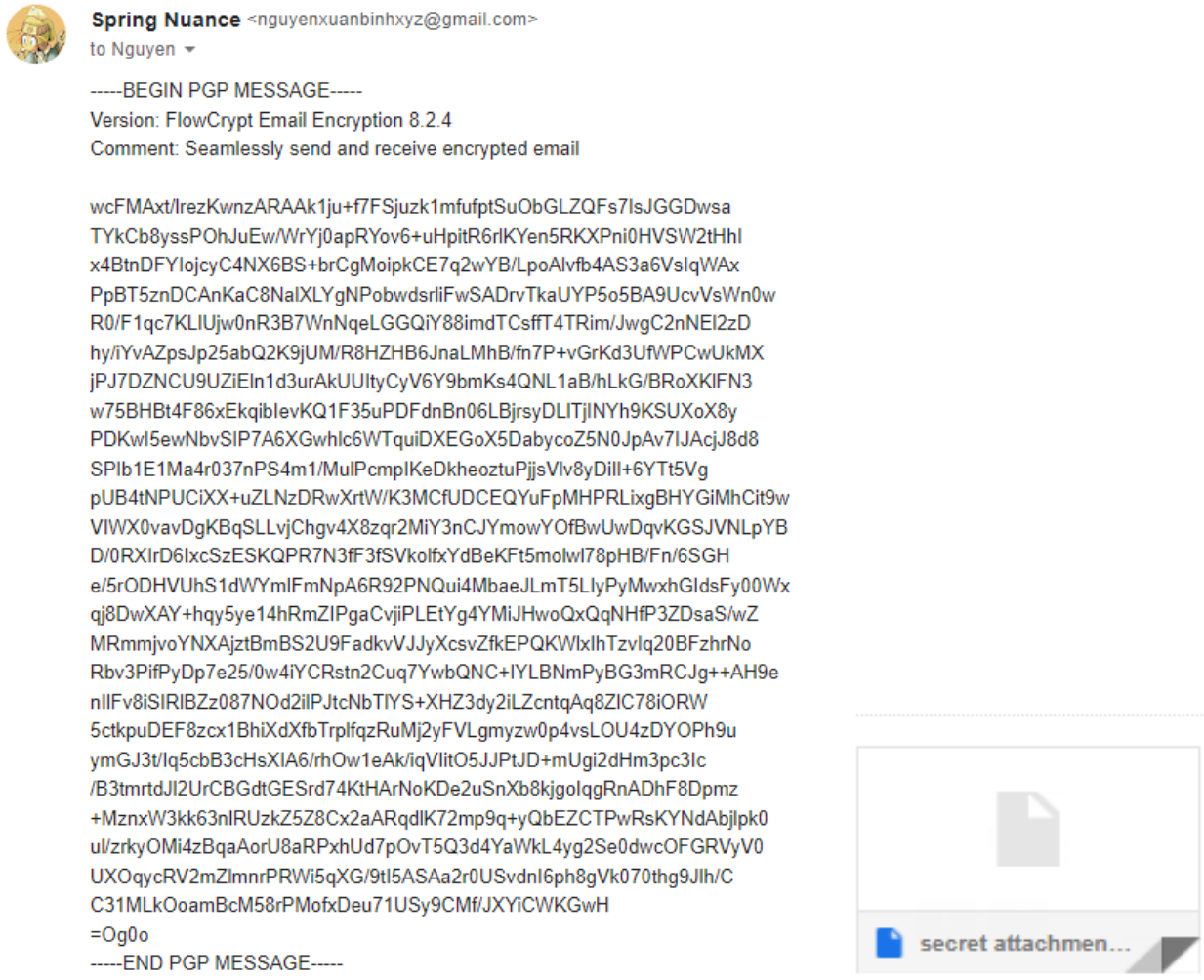


➢ Attachment Encryption

According to FlowCrypt Encryption, both plaintext messages and attachments are protected with end-to-end encryption. Therefore, we proceed to carry out attachment encryption and decryption using FlowCrypt. Now we create a secret plaintext file, called “secret attachment”.



This time, we will send the attachment from nguyenxuanbinhxyz@gmail.com to xuanbinh.dev@gmail.com, indicated by “to Nguyen” next to the profile picture. The attachment is encrypted with xuanbinh.dev@gmail.com public key and the encrypted attachment is:



➢ **Attachment Decryption**

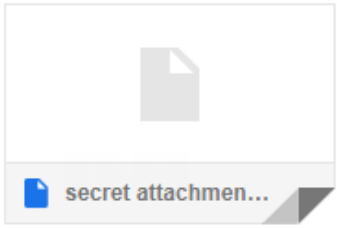
Now we open the mailbox of the account xuanbinh.dev@gmail.com (Nguyen Xuan Binh). Next to the profile picture, “to me” means that this encrypted message has been successfully received by Nguyen Xuan Binh from Spring Nuance.

Spring Nuance

to me

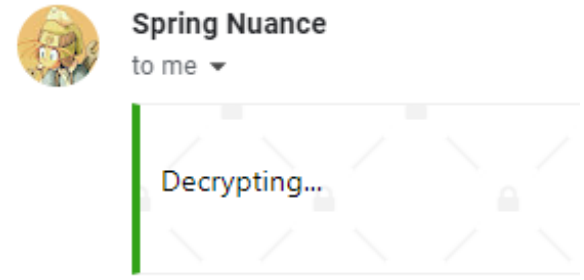
-----BEGIN PGP MESSAGE-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

wcFMAxt/lrezKwnzARAAk1ju+f7FSjuzk1mfufptSuObGLZQFs7lsJGGDwsa
TYkCb8yssPOhJuEw/WrYj0apRYov6+uHpitR6rlKYen5RKXPni0HVSW2tHhl
x4BtnDFYlojcyC4NX6BS+brCgMoipkCE7q2wYB/LpoAlvfb4AS3a6VsIqWAx
PpBT5znDCAnKaC8NalXLYgNPobwdsrliFwSADrvTkaUYP5o5BA9UcvVsWn0w
R0/F1qc7KLlUjw0nR3B7WnNqeLGGQiY88imdTCsffT4TRim/JwgC2nNEl2zD
hy/iYvAZpsJp25abQ2K9jUM/R8HZHB6JnaLMhB/fn7P+vGrKd3UfWPCwUkMX
jPJ7DZNCU9UZiEln1d3urAkUUltyCyV6Y9bmKs4QNL1aB/hLkG/BRoXKlFN3
w75BHBt4F86xEkqiblevKQ1F35uPDFdnBn06LBjrsyDLITjlNYh9KSUXoX8y
PDKwl5ewNbvSIP7A6XGwhlc6WTquiDXEGoX5DabycoZ5N0JpAv7IJAcjJ8d8
SPlb1E1Ma4r037nPS4m1/MulPcmpIKeDkheoztuPjjsVlv8yDill+6YTt5Vg
pUB4tNPUCiXX+uZLNzDRwXrtW/K3MCfUDCEQYuFpMHPRLixgBHYGiMhCit9w
VlWX0vavDgKBqSLLvjChgv4X8zqr2MiY3nCJYmowYOfBwUwDqvKGSJVNLpYB
D/0RXlrD6IxcSzESKQPR7N3fF3fSVkolfxYdBeKFt5molwl78pHB/Fn/6SGH
e/5rODHVUhS1dWYmlFmNpA6R92PNQui4MbaeJLmT5LlyPyMwxhGIdsFy00Wx
qj8DwXAY+hqy5ye14hRmZIPgaCvjiPLEtYg4YMiJHwoQxQqNHfP3ZDsaS/wZ
MRmmjvoYNXAjztBmBS2U9FadkvVJJyXcsvZfkEPQKWlxlhTzvlq20BFzhrNo
Rbv3PifPyDp7e25/0w4iYCRstn2Cuq7YwbQNC+IYLBNmPyBG3mRCJg++AH9e
nIIFv8iSIRlBZz087NOd2ilPJtcNbTlYS+XHZ3dy2iLZcntqAq8ZIC78iORW
5ctkpuDEF8zcx1BhiXdXfbTrplfqzRuMj2yFVLgmyzw0p4vsLOU4zDYOPh9u
ymGJ3t/Iq5cbB3cHsXIA6/rhOw1eAk/iqVlitO5JJPtJD+mUgi2dHm3pc3Ic
/B3tmrtdJl2UrCBGdtGESrd74KtHArNoKDe2uSnXb8kjgolqgRnADhF8Dpmz
+MznxW3kk63nlRUzkZ5Z8Cx2aARqdlK72mp9q+yQbEZCTPwRsKYNdAbjlpk0
ul/zrkyOMi4zBqaAorU8aRPxhUd7pOvT5Q3d4YaWkL4yg2Se0dwcOFGRVyV0
UXOqycRV2mZlmnrPRWi5qXG/9tl5ASAa2r0USvdnl6ph8gVk070thg9Jlh/C
C31MLkOoamBcM58rPMofxDeu71USy9CMf/JXYiCWKGwH
=Og0o
-----END PGP MESSAGE-----

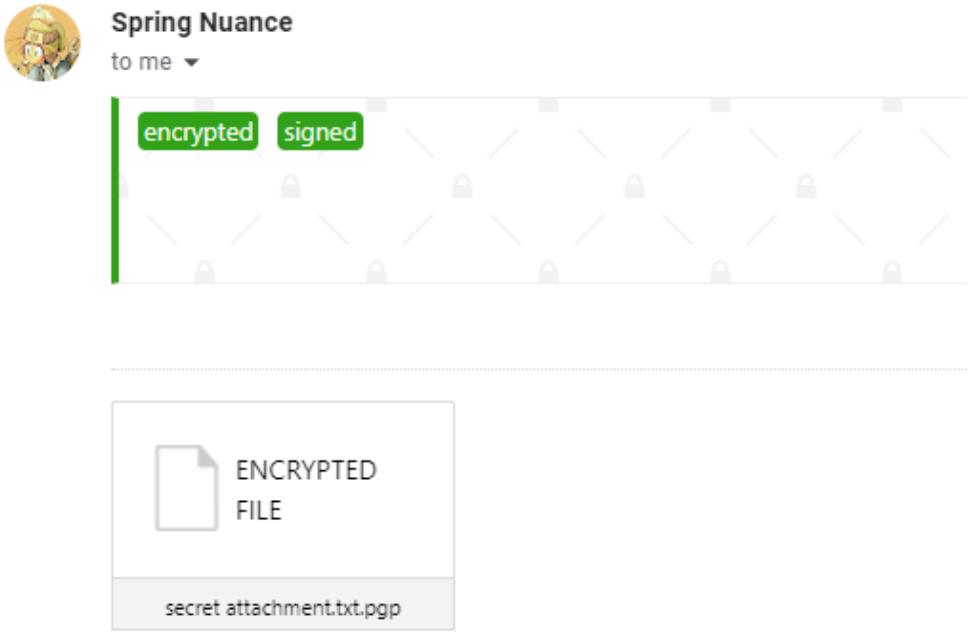


secret attachmen...

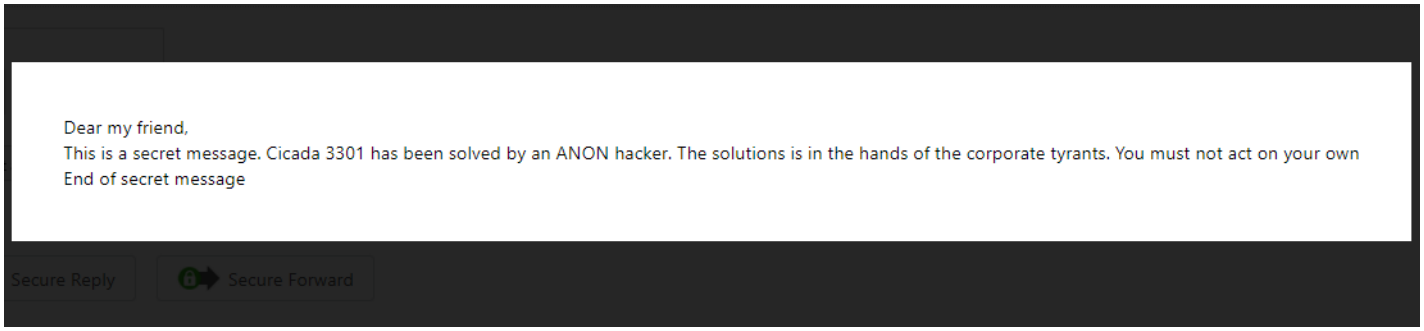
The above encrypted attachment is now decrypted using xuanbinh.dev@gmail.com private key.



The decrypted attachment of the above encrypted attachment is:



The decrypted attachment file now can be downloaded and viewed normally



➢ **Implement Digital Signature from Sender & Receiver**

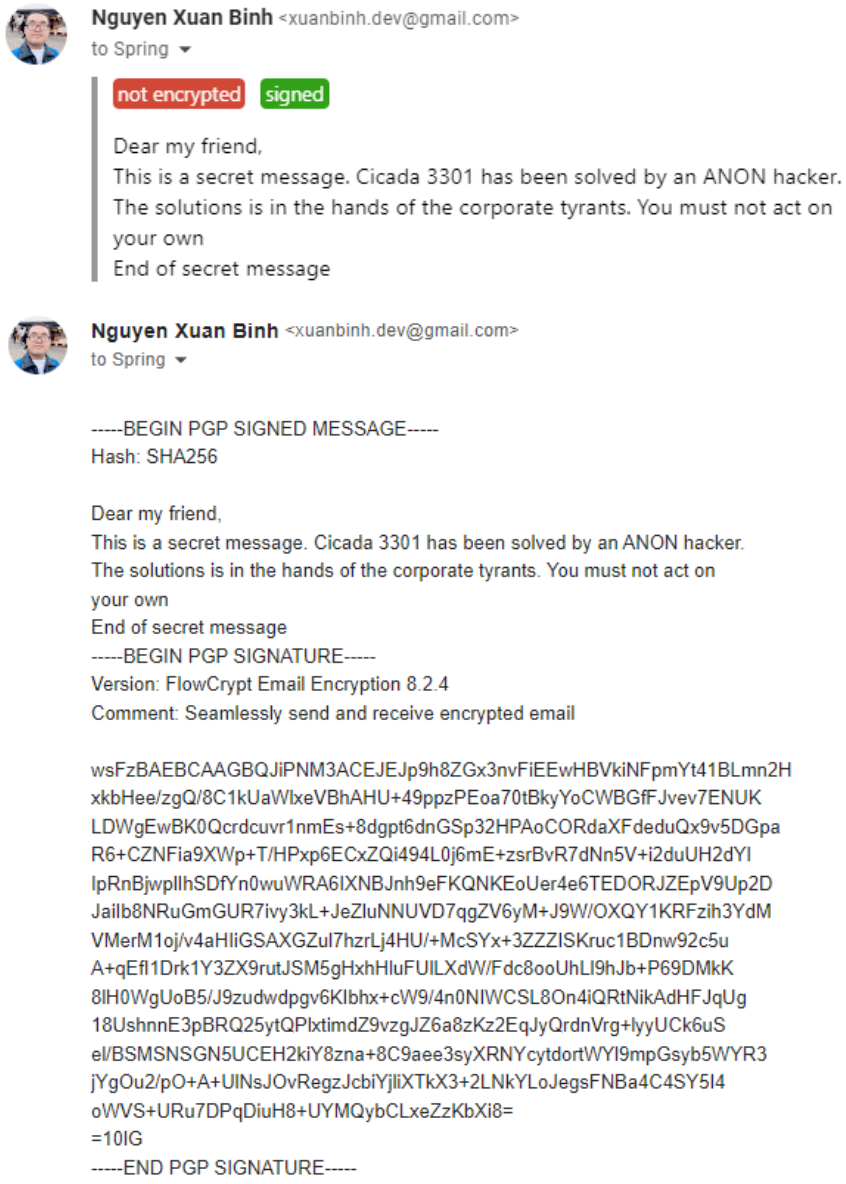
The sender and the receiver are as follows

Sender: xuanbinh.dev@gmail.com (Nguyen Xuan Binh)

Receiver: nguyenxuanbinhxyz@gmail.com (Spring Nuance)

The digital signature is signed by Nguyen Xuan Binh and for the sake of clarity of the digital signature, we choose not to encrypt the message. At the beginning of PGP signed signature, the hashing algorithm FlowCrypt uses is Hash SHA256. The original message is first digested into a hash by SHA-256, and then the hash is encrypted with the sender (Nguyen Xuan Binh) private key, resulting in the final signed digital signature. The digital signature is then attached to the end of the message and sent alongside the message to the receiver.

- **Digital Signature Process from the Sender side**



Nguyen Xuan Binh <xuanbinh.dev@gmail.com>
to Spring

not encrypted signed

Dear my friend,
This is a secret message. Cicada 3301 has been solved by an ANON hacker.
The solutions is in the hands of the corporate tyrants. You must not act on
your own
End of secret message

Nguyen Xuan Binh <xuanbinh.dev@gmail.com>
to Spring

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Dear my friend,
This is a secret message. Cicada 3301 has been solved by an ANON hacker.
The solutions is in the hands of the corporate tyrants. You must not act on
your own
End of secret message
-----BEGIN PGP SIGNATURE-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

wsFzBAEBCAAGBQJiPNM3ACEJEJp9h8ZGx3nvFiEEwHBVkiNFpmYt41BLmn2H
xkbHee/zgQ/8C1kUaWlxeVBhAHU+49ppzPEoa70tBkyYoCWBGfFJvev7ENUK
LDWgEwBK0Qcrdcuvr1nmEs+8dgpt6dnGSp32HPAoCORdaXFdeduQx9v5DGpa
R6+CZNFia9XWp+T/HPxp6ECxZQi494L0j6mE+zsrBvR7dNn5V+i2duUH2dYl
lpRnBjwpllhSDfYn0wuWRA6IXNBJnh9eFKQNKEoUer4e6TEDORJZEpV9Up2D
Jailb8NRuGmGUR7ivy3kL+JeZluNNUVD7qgZV6yM+J9W/OXQY1KRFzih3YdM
VMerM1oj/v4aHliGSAXGZuI7hzrLj4HU/+McSYx+3ZZZISKruc1BDnw92c5u
A+qEfl1Drk1Y3ZX9rutJSM5gHxhHluFUlLXdW/Fdc8ooUhLI9hJb+P69DMkK
8lH0WgUoB5/J9zudwdpgv6KIbhx+cW9/4n0NIWCSL8On4iQRtNikAdHFJqUg
18UshnnE3pBRQ25ytQPlxtimdZ9vzgJZ6a8zKz2EqJyQrdnVrg+lyyUCk6uS
el/BSMSNSGN5UCEH2kiY8zna+8C9aee3syXRNYcytdortWYl9mpGsyb5WYR3
jYgOu2/pO+A+UlNsJOvRegzJcbiYjliXTkX3+2LNkYLoJegsFNBa4C4SY5I4
oWVS+URu7DPqDiuH8+UYMQybCLxeZzKbXi8=
=10IG
-----END PGP SIGNATURE-----

Knowledge of the hashing algorithm SHA-256 is required for the receiver to digest the received message into a hash so that they can verify the signature

- **Digital Signature Verification from the Receiver side**

The digital signature and the message is now received by Spring Nuance. He now can see the signature attached at the end of the message. To verify if this message really belongs to Nguyen Xuan Binh and has not been altered, Spring Nuance first digests the raw plaintext with SHA256 into hash1. Now Spring Nuance proceeds to use Nguyen Xuan Binh's public key to decrypt the attached signed signature into hash2

Nguyen Xuan Binh
to me

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Dear my friend,
This is a secret message. Cicada 3301 has been solved by an ANON hacker.
The solutions is in the hands of the corporate tyrants. You must not act on
your own
End of secret message
-----BEGIN PGP SIGNATURE-----
Version: FlowCrypt Email Encryption 8.2.4
Comment: Seamlessly send and receive encrypted email

wsFzBAEBCAAGBQJiPNM3ACEJEJp9h8ZGx3nvFiEEwHBVkiNFpmYt41BLmn2H
xkbHee/zgQ/8C1kUaWlxeVBhAHU+49ppzPEoa70tBkyYoCWBGfFJvev7ENUK
LDWgEwBK0Qcrdcuvr1nmEs+8dgpt6dnGSp32HPAoCORdaXFdeduQx9v5DGpa
R6+CZNFia9XWp+T/HPxp6ECxZQi494L0j6mE+zsrBvR7dNn5V+i2duUH2dYI
IpRnBjwpIlhSDfYn0wuWRA6IXNBJnh9eFKQNKEoUer4e6TEDORJZEpV9Up2D
Jailb8NRuGmGUR7ivy3kL+JeZluNNUVD7qgZV6yM+J9W/OXQY1KRFzih3YdM
VMerM1oj/v4aHliGSAXGZuI7hzrLj4HU/+McSYx+3ZZZISKruc1BDnw92c5u
A+qEfl1Drk1Y3ZX9rutJSM5gHxhHluFUILXdW/Fdc8ooUhLI9hJb+P69DMkK
8lH0WgUoB5/J9zudwdpgv6KIbhx+cW9/4n0NIWCSL8On4iQRtNikAdHFJqUg
18UshnnE3pBRQ25ytQPlxtimdZ9vzgJZ6a8zKz2EqJyQrdnVrg+lyyUCk6uS
el/BSMSNSGN5UCEH2kiY8zna+8C9aee3syXRNYcytdortWYI9mpGsyb5WYR3
jYgOu2/pO+A+UlNsJOvRegzJcbiYjliXTkX3+2LNkYLoJegsFNBa4C4SY5I4
oWVS+URu7DPqDiuH8+UYMQybCLxeZzKbXi8=
=10IG
-----END PGP SIGNATURE-----
```

Since hash1 is equal to hash2, the digital signature has been successfully verified. The message indeed comes from Nguyen Xuan Binh and has not been altered

Nguyen Xuan Binh
to me

> not encrypted signed
>
> Dear my friend,
> This is a secret message. Cicada 3301 has been solved by an ANON hacker.
> The solutions is in the hands of the corporate tyrants. You must not act on
> your own
> End of secret message

=> Conclusion: with the help of PGP software, emails can be sent securely via the networks without worries of spoofing or sniffing. The automatic power of PGP software enables the seamless process of encryption, decryption and digital signatures, which helps users compose secure emails as simple as normal emails without PGP.