Secure File Transfer Usage Guide

Overview & Goal:

How do you transfer a password protected file to a geographically separated partner over the internet? You need to securely transfer the password over the internet too. This task is not straightforward, but it is doable. Believe it or not a secret password can be shared across a public network where every exchange is being recorded by untrusted 3rd parties. Yet only the two communicating can derive the meaning of the message.

This strategy does not depend on any kind of 'End to end' encryption provided by a third party's servers. No external servers are required, though they can be used during file handoff (ex. Email inboxes or file sharing services). The recent events from popular communication platforms like Zoom and Whatsapp have proven that 3rd party server-based communications cannot be trusted on their end-to-end encryption promises.

Core concept – *key pairs*

This setup is based on 'Public Key Cryptography'. It is a deep subject, but all you really need to know is this: Each person has a pair of codes called a keypair. These keypairs are different than traditional physical keys. Once one key of the pair is used to scramble a message, only the other key from the same pair can unscramble the message. One code is called the private key. The other is called the public key. The trick to security with keypairs is how we cleverly use them.

Keypairs are very handy for security when shared using 2 simple rules. The most important rule is **'NEVER SHARE YOUR PRIVATE KEY!'** Whoever holds your private key can open any files locked by your public key. If your private key becomes known, all security of that keypair is lost. The other rule of keypair sharing is 'Share your public key with your communication partner'. When you share your public key with a partner, you have given them the ability to lock files in a way that only you can unlock, because only you hold the private key of the pair. Really the whole world can know your public key without any harm. Some could try to impersonate the trusted party you shared your public key with, but we will cover that more later.

Using keypairs in practice

In practice, keypair based crypto is impractically slow and unnecessary for large messages and files. The solution to this problem is simple: Make up a very strong temporary password, encrypt your secret payload using this password, then use the recipient's public key to scramble the very strong password. The payload and scrambled password can be securely sent over any unsecured channel safely, because only the holder of the private key from the pair can unscramble the strong password and unlock the payload.

A Secure File Transfer Workflow

1) **Initial Setup (done once for each communication partner)**
   a) **Generate a keypair.**
   b) **Exchange public keys with your partner.**

2) **Sending a Secured Payload**
   a) **Generate a Strong Password**
   b) **Lock the Payload with the Strong Password**
   c) **Scramble the Password with the Partner's Public Key**
   d) **Discard the Strong Password**
   e) **Deliver the payload and scrambled password to your partner**

3) **Unpacking a received payload**
   a) **Unscramble the strong password using your private key**
   b) **Apply the password to unlock the payload**

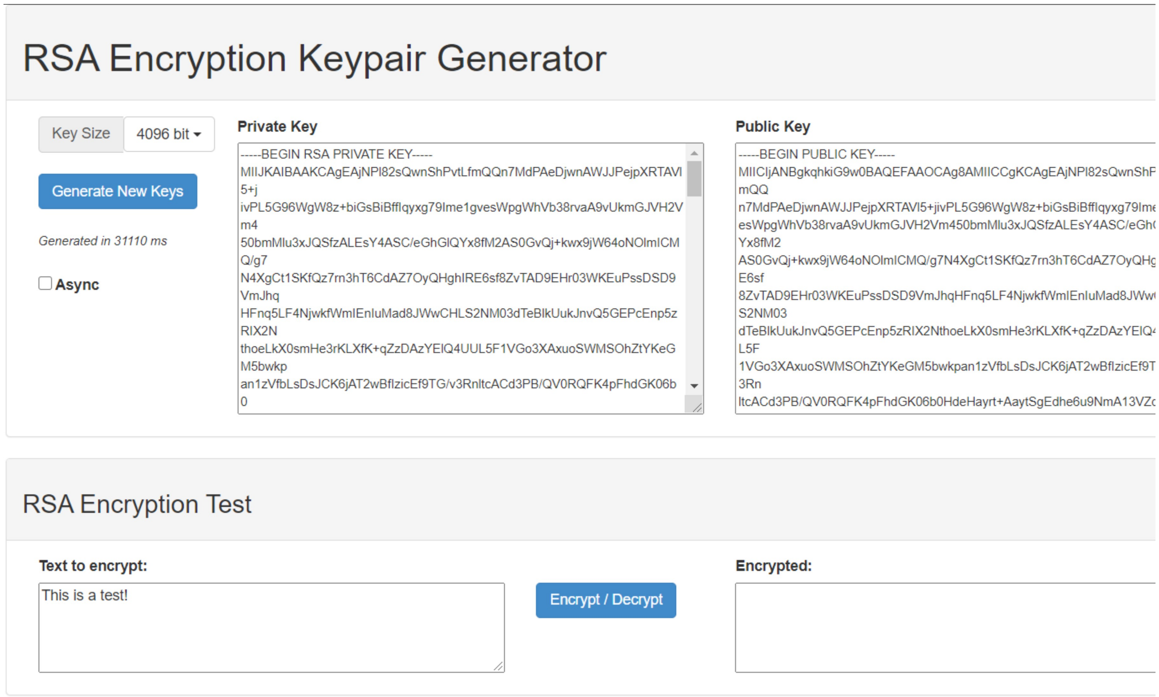
The same keypair can be re-used to scramble new unique passwords for each secured payload, as long as both partners keep their private keys secret. Each password and its scrambled version should never be re-used for future payloads.

Detailed Steps

1) Initial Setup (done once for each partner)

a) Generate a keypair.

Open ‘Key Generator.html’ and hang tight, the new keys can take up to 1 minute to appear. The internet is not required for any of these steps. All computation is done locally. Ideally the computer used for this process is permanently disconnected from the internet. Payloads can be loaded from portable media.



Key Size 4096 bit

Generated in 31110 ms

□ Async

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAjNPl82sQwnShPvtLfmQQn7MdPAeDjwnAWJJPejpXRTAVl
5+j
ivPL5G96WgW8z+biGsBiBfflqyxg79Ime1gvesWpgWhVb38rvaA9vUkmGJVH2V
m4
50bmMlu3xJQSfzALEsY4ASC/eGhGlQYx8fM2AS0GvQj+kwx9jW64oNOlmICM
Q/g7
N4XgCt1SKfQz7rn3hT6CdAZ7OyQHghlRE6sf8ZvTAD9EHr03WKEuPssDSD9
VmJhq
HFnq5LF4NjwkfWmlEnIuMad8JWwCHLS2NM03dTeBlkUukJnvQ5GEPcEnp5z
RIX2N
thoeLkX0smHe3rKLXfK+qZzDAzYElQ4UUL5F1VGo3XAxuoSWMSOhZtYKeG
M5bwkp
an1zVfbLsDsJCK6jAT2wBfIzicEf9TG/v3RnltcACd3PB/QV0RQFK4pFhdGK06b
0
```

Public Key

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAjNPl82sQwnShP
mQQ
n7MdPAeDjwnAWJJPejpXRTAVl5+jivPL5G96WgW8z+biGsBiBfflqyxg79Ime
esWpgWhVb38rvaA9vUkmGJVH2Vm450bmMlu3xJQSfzALEsY4ASC/eGh
Yx8fM2
AS0GvQj+kwx9jW64oNOlmICMQ/g7N4XgCt1SKfQz7rn3hT6CdAZ7OyQHg
E6sf
8ZvTAD9EHr03WKEuPssDSD9VmJhqHFnq5LF4NjwkfWmlEnIuMad8JWw
S2NM03
dTeBlkUukJnvQ5GEPcEnp5zRIX2NthoeLkX0smHe3rKLXfK+qZzDAzYElQ4
L5F
1VGo3XAxuoSWMSOhZtYKeGM5bwkpan1zVfbLsDsJCK6jAT2wBfIzicEf9T
3Rn
ltcACd3PB/QV0RQFK4pFhdGK06b0HdeHayrt+AaytSgEdhe6u9NmA13VZ
```

Text to encrypt:

This is a test!

Encrypted:

Once the keypair has been generated, copy/paste and save these public and private key codes into their own new text files. Give both descriptive names like ‘AndrewsPublickey.txt’ and ‘AndrewsPrivateKey.txt’ so you don’t accidentally reveal your private key. I suggest marking these files as Read only under file preferences to prevent editing the keys and ruining them. Protect your keys, **especially the private key**, or all security is lost!

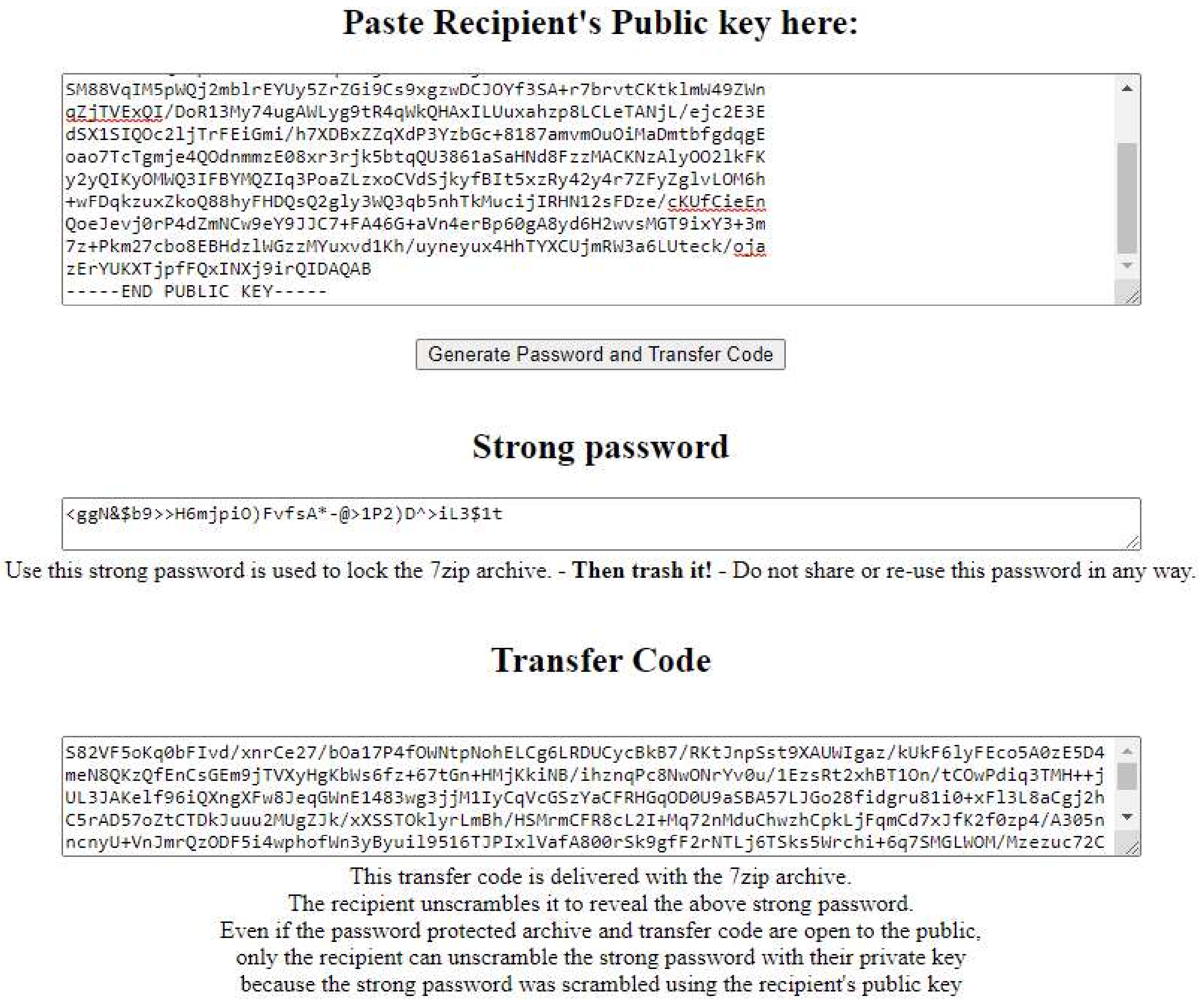
b) Exchange public keys with your partner.

Any open channel is ok, but keep in mind you are alerting the public that an encryption key is being exchanged. Sending your public key is best done as discretely as possible.

2) Sending a secured File

a) Generate a strong password

Open '*Package_Payload.html*'
Replace the default public key with the recipient's public key.
Click the 'Generate Password and Transfer Code' button.



Paste Recipient's Public key here:

```
SM88VqIM5pWQj2mblrEYUy5ZrZGi9Cs9xgzwDCJOYf3SA+r7brvtCKtklmW49ZWn
qZjTVExQI/DoR13My74ugAWLyg9tR4qWkQHAxILUuxahzp8LCLeTANjL/ejc2E3E
dSX1SIQOc2ljTrFEiGmi/h7XDBxZZqXdP3YzbGc+8187amvmOuOiMaDmtbfgdqgE
oao7TcTgmje4QOdnmmzE08xr3rjk5btqQU3861aSaHNd8FzzMACKNzAlyOO2lkFK
y2yQIKyOMWQ3IFBYMQZIq3PoaZLzxoCVdSjkyfBIt5xzRy42y4r7ZFyZglvLOM6h
+wFDqkzuxZkoQ88hyFHDQsQ2gly3WQ3qb5nhTkMucijIRHN12sFDze/cKUfCieEn
QoeJevj0rP4dZmNCw9eY9JJC7+FA46G+aVn4erBp60gA8yd6H2wvsMGT9ixY3+3m
7z+Pkm27cbo8EBHdzlWGzzMYuxvd1Kh/uyneyux4HhTYXCUjmRW3a6LUteck/oja
zErYUKXTjpfFQxINXj9irQIDAQAB
-----END PUBLIC KEY-----
```

Strong password

```
<ggN&$b9>>H6mjpiO)FvfsA*-@>1P2)D^>iL3$1t
```

Use this strong password is used to lock the 7zip archive. - **Then trash it!** - Do not share or re-use this password in any way.

Transfer Code

```
S82VF5oKq0bFIvd/xnrCe27/bOa17P4fOWNtpNohELCg6LRDUCycBkB7/RKtJnpSst9XAUWIgaz/kUkF6lyFEco5A0zE5D4
meN8QKzQfEnCsGEm9jTVXyHgKbWs6fz+67tGn+HMjKkiNB/ihznqPc8NwONrYv0u/1EzsRt2xhBT1On/tCOwPdiq3TMH++j
UL3JAKelf96iQXngXFw8JeqGWnE1483wg3jjM1IyCqVcGSzYaCFRHGqOD0U9aSBA57LJGo28fidgru81i0+xFl3L8aCgj2h
C5rAD57oZtCTDkJuuu2MUgZJk/xXSSTOklyrLmBh/HSMrmCFR8cL2I+Mq72nMduChwzhCpkLjFqmCd7xJfK2f0zp4/A305n
ncnyU+VnJmrQzODF5i4wphofWn3yByuil9516TJPIxlVafA800rSk9gfF2rNTLj6TSks5Wrchi+6q7SMGLWOM/Mzezuc72C
```

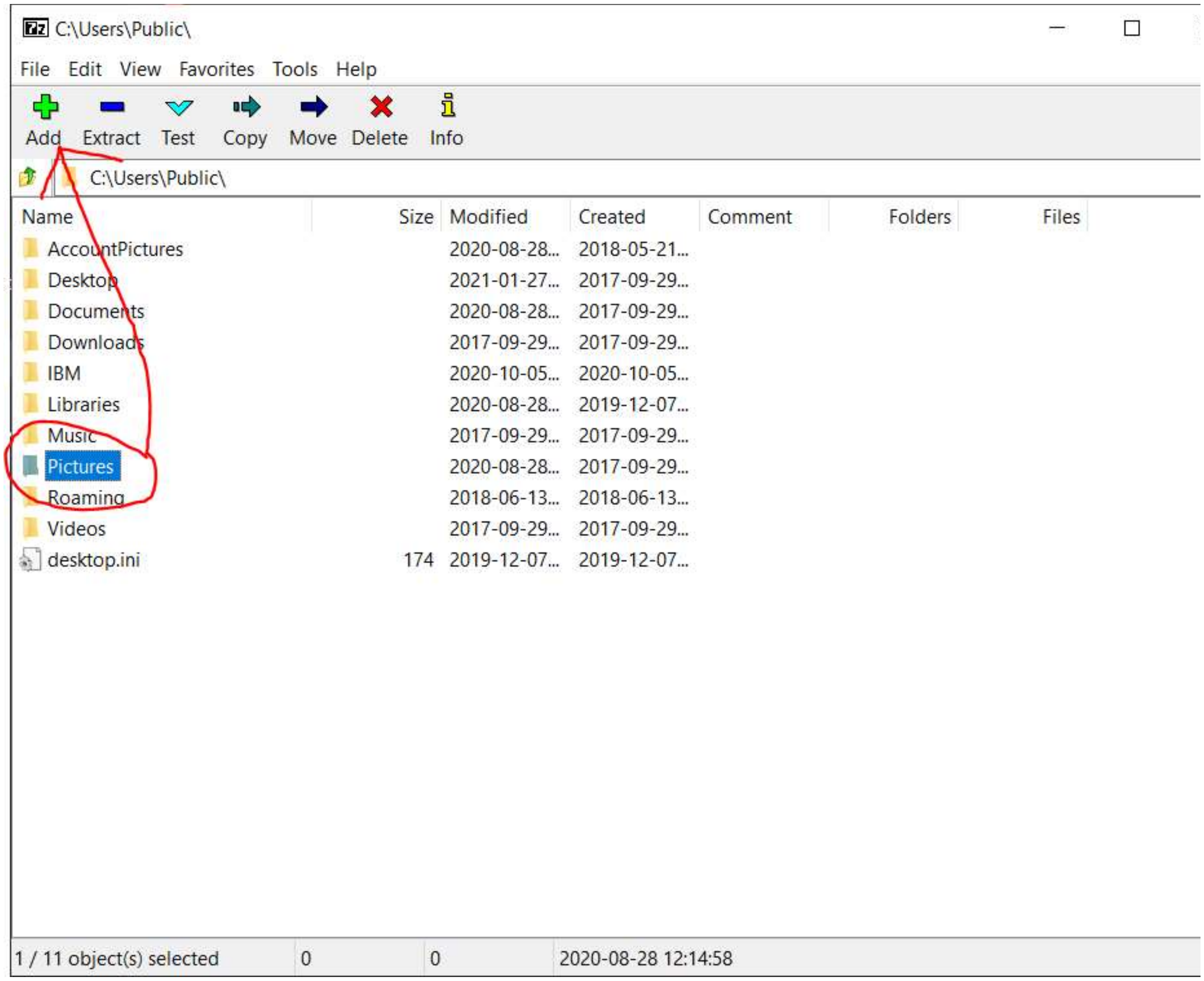
This transfer code is delivered with the 7zip archive.
The recipient unscrambles it to reveal the above strong password.
Even if the password protected archive and transfer code are open to the public,
only the recipient can unscramble the strong password with their private key
because the strong password was scrambled using the recipient's public key

b) Lock the payload with the strong password

Open '7Zip_portable.exe'

Select the file or folder you want to send.

Press the 'Add' button.



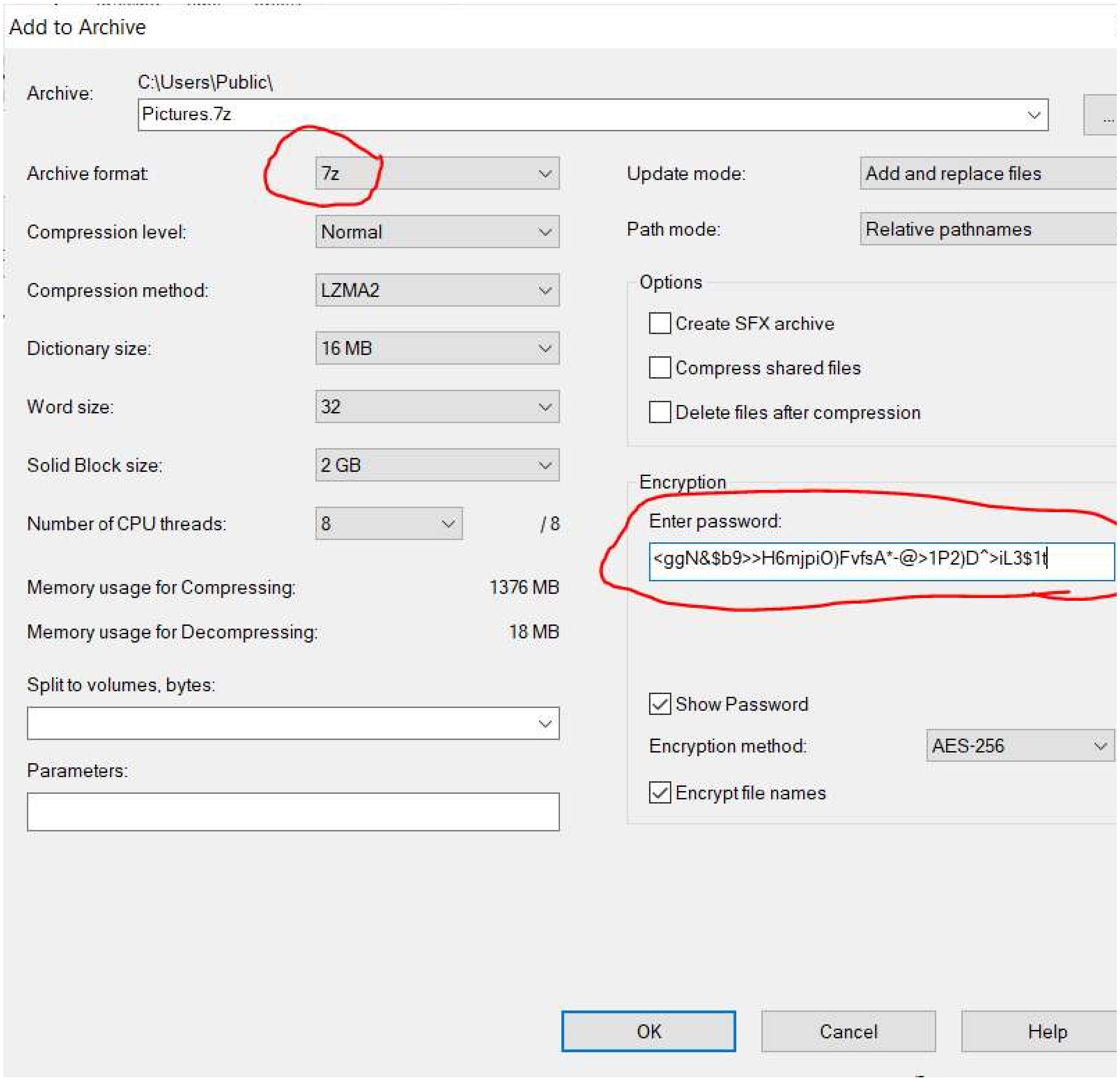
Name	Size	Modified	Created	Comment	Folders	Files
AccountPictures		2020-08-28...	2018-05-21...			
Desktop		2021-01-27...	2017-09-29...			
Documents		2020-08-28...	2017-09-29...			
Downloads		2017-09-29...	2017-09-29...			
IBM		2020-10-05...	2020-10-05...			
Libraries		2020-08-28...	2019-12-07...			
Music		2017-09-29...	2017-09-29...			
Pictures		2020-08-28...	2017-09-29...			
Roaming		2018-06-13...	2018-06-13...			
Videos		2017-09-29...	2017-09-29...			
desktop.ini	174	2019-12-07...	2019-12-07...			

1 / 11 object(s) selected | 0 | 0 | 2020-08-28 12:14:58

Set the archive format to '7z'

paste the Strong Password into the encryption section

click 'OK'



Archive: C:\Users\Public\Pictures.7z

Archive format: 7z

Compression level: Normal

Compression method: LZMA2

Dictionary size: 16 MB

Word size: 32

Solid Block size: 2 GB

Number of CPU threads: 8 / 8

Memory usage for Compressing: 1376 MB

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Update mode: Add and replace files

Path mode: Relative pathnames

Options

□ Create SFX archive

□ Compress shared files

□ Delete files after compression

Encryption

Enter password:

<ggN&$b9>>H6mjpiO)FvfsA*-@>1P2)D^>iL3$1t

☑ Show Password

Encryption method: AES-256

☑ Encrypt file names

c) Scramble the password with the partner’s public key

This is already done on the '*Package_Payload.html*' page. Simply include the Transfer Code with your secured transmission.

d) Discard the strong password

There is no reason to keep the strong password. That only leaves it open to be stolen.

e) Deliver the payload and scrambled password to your partner

Email, dropbox, usb drive in the mail, whatever. Just remember that being discreet is preferred. It is obvious you are exchanging encrypted messages.

3) Unpacking a received payload

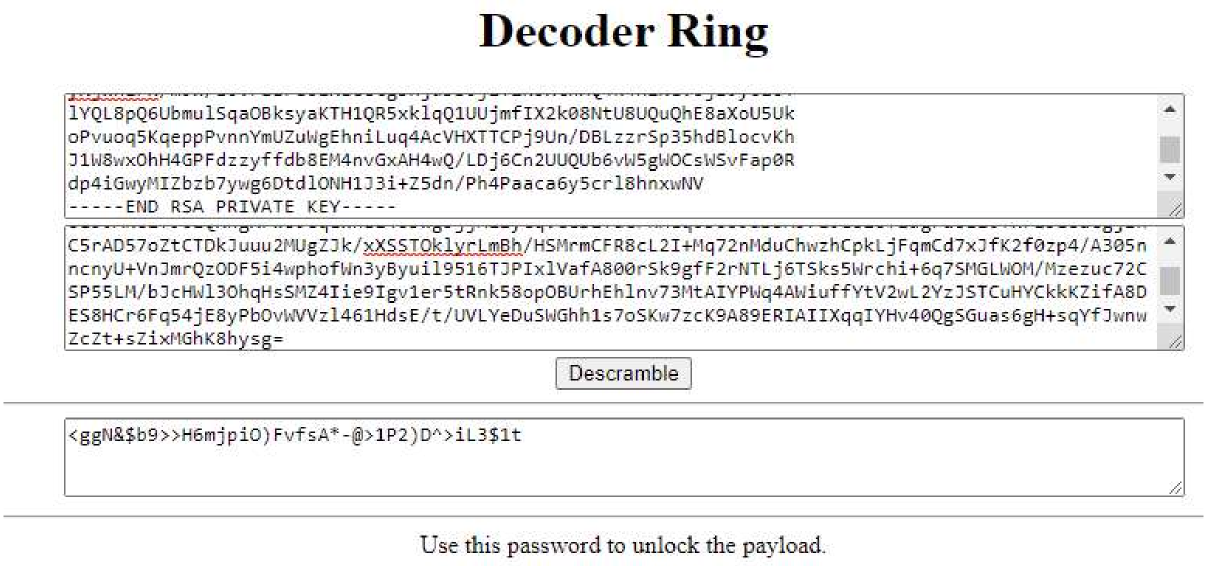
a) Unscramble the strong password using your private key

Open *'Receive_Payload.html'*

Paste you private key in the top box

Paste the scrambled password in the middle box

Press the 'Descramble' button



Decoder Ring

```
1YQL8pQ6UbmulSqaOBksyaKTH1QR5xklqQ1UUjmfIX2k08NtU8UQuQhE8aXoU5Uk
oPvuoq5KqeppPvnnYmUZuWgEhniLuq4AcVHXTTCPj9Un/DBLzzrSp35hdBlocvKh
J1W8wxOhH4GPFdzzyffdb8EM4nvGxAH4wQ/LDj6Cn2UUQUb6vW5gWOCsWSvFap0R
dp4iGwyMIZbzb7ywg6DtdlONH1J3i+Z5dn/Ph4Paaca6y5crl8hnxwNV
-----END RSA PRIVATE KEY-----
```

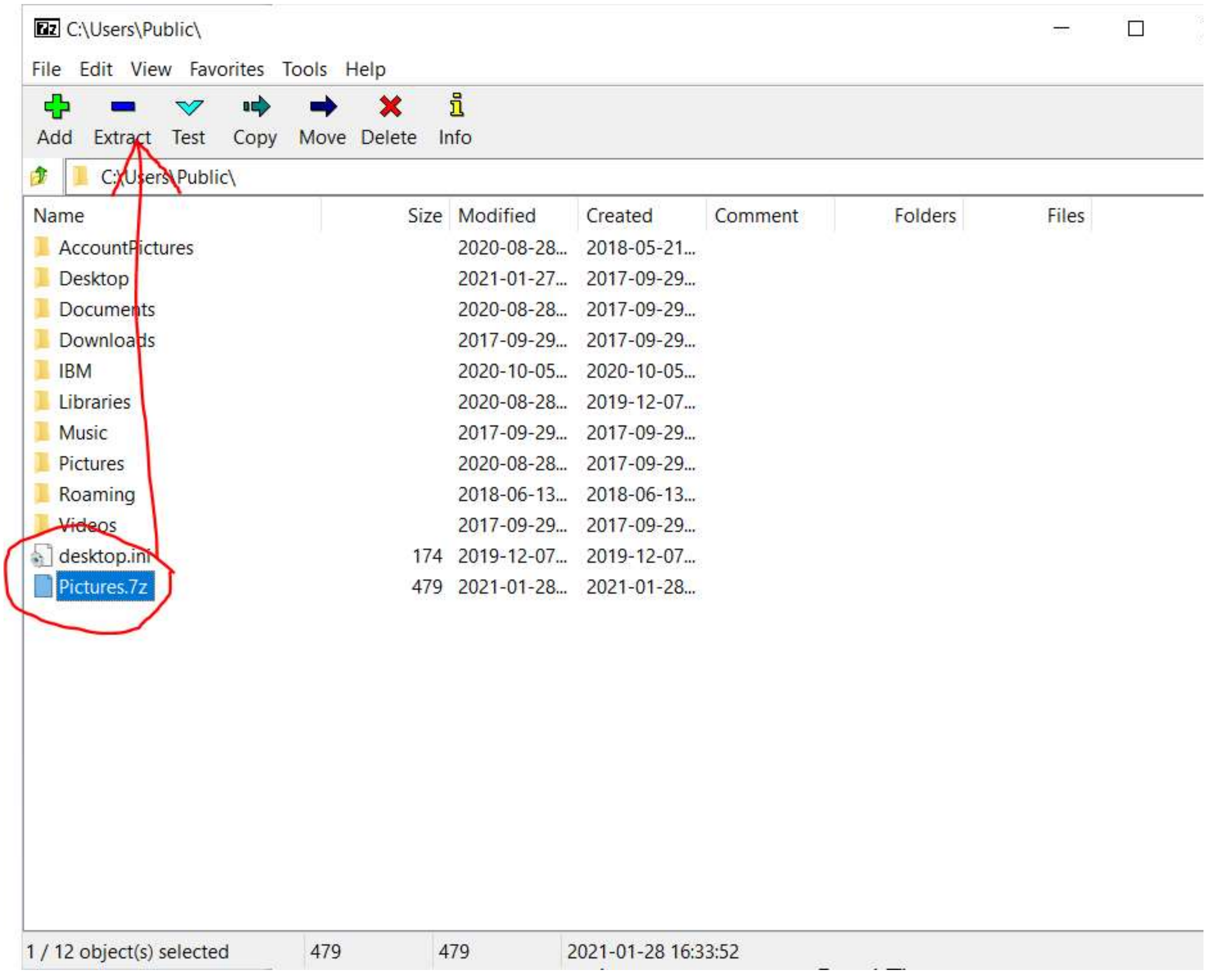
```
C5rAD57oZtCTDkJuuu2MUgZJk/xXSSTOklyrLmBh/HSMrmCFR8cL2I+Mq72nMduChwzhCpkLjFqmCd7xJfK2f0zp4/A305n
ncnyU+VnJmrQzODF5i4wphofWn3yByuil9516TJPIxlVafA800rSk9gfF2rNTLj6TSks5Wrchi+6q7SMGLWOM/Mzezuc72C
SP55LM/bJcHWl3OhqHsSMZ4Iie9Igv1er5tRnk58opOBUrhEhlnv73MtAIYPWq4AWiuffYtV2wL2YzJSTCuHYCkkKZifA8D
ES8HCr6Fq54jE8yPbOvWVVzl461HdsE/t/UVLYeDuSWGhh1s7oSKw7zcK9A89ERIAIIXqqIYHv40QgSGuas6gH+sqYfJwnw
ZcZt+sZixMGhK8hysg=
```

```
<ggN&$b9>>H6mjpiO)FvfsA*-@>1P2)D^>iL3$1t
```

Use this password to unlock the payload.

g) Apply the password to unlock the payload

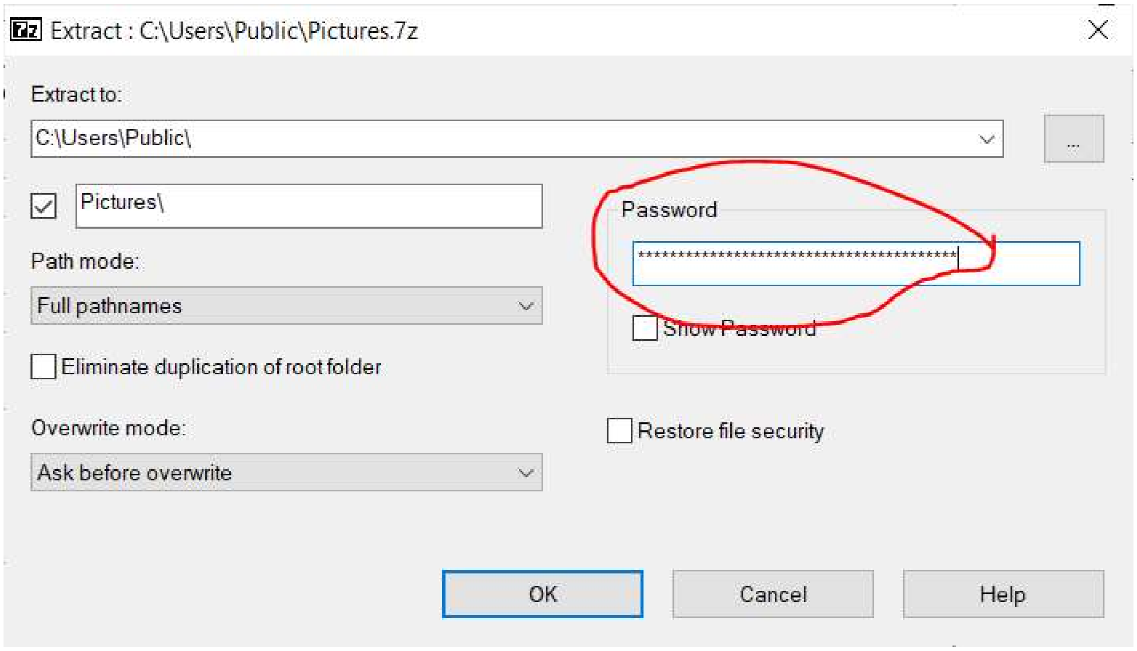
Extract the .7z file using 7zip_portable.exe



Name	Size	Modified	Created	Comment	Folders	Files
AccountPictures		2020-08-28...	2018-05-21...			
Desktop		2021-01-27...	2017-09-29...			
Documents		2020-08-28...	2017-09-29...			
Downloads		2017-09-29...	2017-09-29...			
IBM		2020-10-05...	2020-10-05...			
Libraries		2020-08-28...	2019-12-07...			
Music		2017-09-29...	2017-09-29...			
Pictures		2020-08-28...	2017-09-29...			
Roaming		2018-06-13...	2018-06-13...			
Videos		2017-09-29...	2017-09-29...			
desktop.ini	174	2019-12-07...	2019-12-07...			
Pictures.7z	479	2021-01-28...	2021-01-28...			

1 / 12 object(s) selected 479 479 2021-01-28 16:33:52

Enter the unscrambled strong password to unlock the payload.



Extract : C:\Users\Public\Pictures.7z

Extract to: C:\Users\Public\

☑ Pictures\

Path mode: Full pathnames

□ Eliminate duplication of root folder

Overwrite mode: Ask before overwrite

Password

****

□ Show Password

□ Restore file security