AUTHENTICATION

In order for you to be able to ensure the messages we publish on the various blogs and social networking sites have not been compromised or forged, you will need to familiarize yourself with the concept of "PUBLIC KEY CRYPTOGRAPHY," and download the trial version and our PUBLIC KEYS.

Our purposes for using PUBLIC KEY CRYPTOGRAPHY are pretty straightforward. We want you to be able to have a means of verifying the communications we publish and be able to do so with the sophistication of military-grade encryption. PUBLIC KEY CRYPTOGRAPHY also allows us to remain anonymous while preventing imposters from corrupting our message.

Here is a basic outline on how it works:

We have each created a “KEYPAIR” consisting of two unique, but related, parts. The first part is the PUBLIC KEY, which is widely published and the part you download to your computer. The second part is a SECRET KEY, which is kept confidentially by us. That SECRET KEY is also encrypted with a pass phrase that is known only to us.

PUBLIC/SECRET KEYPAIRS are mathematically related, but it is impossible to derive the SECRET KEY from the PUBLIC KEY. The functions of the PUBLIC KEY are only possible when dealing with the corresponding SECRET KEY and the functions of the SECRET KEY are only possible when dealing with the corresponding PUBLIC KEY.

Authentication

The PUBLIC KEY has two important functions: encryption and verification.
The SECRET KEY has two important functions: decryption and signing.

The encryption function is the means by which someone can encrypt a message or file that only the holder of the corresponding SECRET KEY (along with the pass phrase) can decrypt. This is very handy when sending confidential messages or files along an unsecured medium (such as the internet). Once you encrypt a file with a PUBLIC KEY, only the person with the corresponding SECRET KEY can read it. We don’t anticipate you will be using our PUBLIC KEYS to send us messages due to the nature of the operation.

The verification function is the one you will be using the most often. The PUBLIC KEY is used to verify the unique digital signature that is only possible to make by using the corresponding SECRET KEY. Once we sign the communications with our SECRET KEY(S) and publish them on the various websites, you will be able to verify that those documents came from us and have not been corrupted, altered, or forged by using our PUBLIC KEY(S).

You will also note that we have each published our PUBLIC KEYS and that we have each signed each others’ keys. This will prevent a hacker from impersonating our keys. If someone were to attempt to forge a key, it would lack all of the unique digital fingerprints and all of our signatures.

All of our PUBLIC KEYS are published in multiple places on the internet. They are stored in GOOGLE, and the PGP Global Directory. You will find links to our keys on the blogs, and social networking sites. PUBLIC KEYS can also be transmitted in block text form. This form may also be published on FACEBOOK and the blogs, should the need arise..

We have listed the unique digital fingerprints for all 4 of our keys. This fingerprint can also be used to verify that you have the correct keys.

In order to use the PUBLIC KEY CRYPTOGRAPHY functions, you will need to download the trial version (or purchase an upgrade from PGP Corporation). The functionality of the trial version is sufficient for our purposes, but we would encourage you to explore the functions of PGP and consider buying a copy. Please note that PGP Corporation has no association with The Committee nor do they have any knowledge, endorse or oppose what we are doing.

Authentication

It is not necessary for everyone to use PGP to verify the validity of the files. Most people will be able to participate without using PGP or verifying the files. It is only necessary for enough people to do so, and to make enough noise should they find a corrupted message, that others will know. Those who elect not to use this feature will have to rely upon those that do.

When you launch the PGP trial version, you will be prompted to create your own key pair. Please do so. This will enable you to sign your copies of our PUBLIC KEYS and add even more security to the process.

The trial version will also allow you to “import” our PUBLIC KEYS from all the various sources and store them on your PGP “keyring.” This step is essential for you to use the verification functions of our PUBLIC KEY.

If you wish to read more on the features of PUBLIC KEY CRYPTOGRAPHY, we would encourage you to download the explanation from the PGP Corporation.

The format we will use on the blogs and social networking sites will be to have the normal entries as you would expect, and then mirror the information with a .DOC, .PDF, or some other relevant file that bears one or more of our signatures. Not all entries will be mirrored. Any one signature from us with an official digital signature is sufficient for it to be authentic. One valid signature carries the weight of all four. Each one of us speaks for all of us, but we also have schedules to keep and operational security measures to observe.

Of the two methods for digital authentication available, we will mostly use a DETACHED SIGNATURE, which is a separate file from the signed file. By activating the signature file, you will be prompted to browse to the relevant file. If the signature matches the file, the signature is considered valid and PGP will inform you of such. If anything in the file has been altered (one period, space, word, etc.), PGP will show that it is a “bad signature.”

We will link a .zip file with current documents along with the corresponding signatures. The .zip file itself will have a signature. Any succeeded or outdated files will be removed from the active .zip. This will simplify how the current files and documents can be verified.

Authentication

Here are the photographs, serial numbers, hexadecimal and biometric fingerprints for our keys. You can verify the keys you download from OPERATIONORANGE.org, or the PGP GLOBAL DIRECTORY.

Mr. Brown

0xB61A6589

6C92 4B81 06BE 2CC5 6E4E 5A75 8A7C E990 B61A 6589

glucose misnomer dragnet inventive afflict racketeer Burbank resistor goldfish distortion enlist impartial Oakland informant treadmill millionaire Scotland Bradbury fracture matchmaker

Mr. Green

0xA2DD064D

7B41 17BA 8DAF 77B0 C772 BF45 6BF1 C68F A2DD 064D

kickoff decadence banjo puberty optic pharmacy involve phonetic soybean holiness slingshot detector glitter vacancy southward midsummer rebirth tambourine afflict disruptive

Mr. Black

0x91CCE24D

CBC0 B494 3E9C 807A 1B63 2DE0 587A 7F03 91CC E24D

spheroid recipe scenic molecule concert October merit infancy beeswax Galveston button tobacco endorse infancy lockup aggregate pheasant revolver tiger disruptive

Ms. Plum

0x773C34F6

0B38 568E 515D 8F7C 5A51 3AEA 5E20 9DBF 773C 34F6

alone consulting egghead microwave drunken filament payday informant enlist enchanting cleanup undaunted eyeglass butterfat quadrant rebellion involve crossover choking vocalist

LINKS TO PGP RELATED SITES

Symantec / PGP Corporation
http://www.symantec.com/business/theme.jsp?themeid=pgp

PGP Trialware - refer to the sidebar on OPERATIONORANGE.org for the most current link. Trialware is located under “WHOLE DISK ENCRYPTION” under the “BUSINESS” software section of the Symantec website. Follow the instructions for the download of PGP DESKTOP 10.1.0.

To get the PGP Trial version, go to the Symantec website, and follow the following to get to the trial version of PGP Whole Disk Encryption:

- - -Select "Business" from the top masthead
- - -Select "Products" - "Products A-Z"
- - -Scroll down and select"Whole Disk Encryption"
- - -Click on "Trialware"
- - -Click on "PGP Whole Disk Encryption Trialware"

Follow the directions for download. Site registration is required. Download is free after registration. This will enable you to receive the trialware licensing code. Note that some functionality will disable after the trial period, but the "keys" function will remain active after the trial is over.

PGP Global Directory
https://keyserver.pgp.com/vkd/GetWelcomeScreen.event

PGP Public Key Cryptography Explanation
http://en.wikipedia.org/wiki/Pretty_Good_Privacy

Public Keys for The Committee
http://operationorange.org/keys.zip

Note that PGP Corporation is now owned by Symantec Corporation.