# Deniable encryption

In cryptography and steganography, plausibly **deniable encryption** is encryption that allows its users to convincingly deny that some specific encrypted data exists,[1] that a given piece of data is encrypted, or that they are able to decrypt a given piece of encrypted data[*citation needed*]. Such denials may or may not be genuine. For example, although suspicions might exist that the data is encrypted, it may be impossible to prove it without the cooperation of the users. If the data is encrypted, the users genuinely may not be able to decrypt it. Deniable encryption serves to undermine an attacker's confidence either that data is encrypted, or that the person in possession of it can decrypt it and provide the associated plaintext.

Normally ciphertexts decrypt to a single plaintext and hence once decrypted, the encryption user cannot claim that he encrypted a different message. Deniable encryption allows its users to decrypt the ciphertext to produce a different (innocuous but plausible) plaintext and insist that it is what they encrypted. The holder of the ciphertext will not have the means to differentiate between the true plaintext, and the bogus-claim plaintext.

## Function

Deniable encryption allows an encrypted message to be decrypted to different sensible plaintexts, depending on the key used, or otherwise makes it impossible to prove the existence of the real message without the proper encryption key. This allows the sender to have plausible deniability if compelled to give up his or her encryption key. The notion of "deniable encryption" was used by Julian Assange and Ralf Weinmann in the Rubberhose filesystem[2] and explored in detail in a paper by Ran Canetti, Cynthia Dwork, Moni Naor, and Rafail Ostrovsky in 1996.

### Scenario

Deniable encryption allows the sender of an encrypted message to deny sending that message. This requires a trusted third party. A possible scenario works like this:

1. Bob suspects his wife Alice is engaged in adultery. That being the case, Alice wants to communicate with her secret lover Carl. She creates two keys, one intended to be kept secret, the other intended to be sacrificed. She passes the secret key (or both) to Carl.
2. Alice constructs an innocuous message M1 for Carl (intended to be revealed to Bob in case of discovery) and an incriminating love letter M2 to Carl. She constructs a cipher-text C out of both messages M1, M2 and emails it to Carl.
3. Carl uses his key to decrypt M2 (and possibly M1, in order to read the fake message, too).
4. Bob finds out about the email to Carl, becomes suspicious and forces Alice to decrypt the message.
5. Alice uses the sacrificial key and reveals the innocuous message M1 to Bob. Since Bob does not know the other key, he has to assume that there is no other message M2.

Another possible scenario involves Alice sending the same ciphertext (some secret instructions) to Bob and Carl, to whom she has handed different keys. Bob and Carl are to receive different instructions and must not be able to read each other's instructions. Bob will receive the message first and then forward it to Carl.

1. Alice constructs the ciphertext out of both messages, M1 and M2, and emails it to Bob.
2. Bob uses his key to decrypt M1 and isn't able to read M2.
3. Bob forwards the ciphertext to Carl.
4. Carl uses his key to decrypt M2 and isn't able to read M1.

## Modern forms of deniable encryption

Modern deniable encryption techniques exploit the pseudorandom permutation properties of existing block ciphers, making it cryptographically infeasible to prove that the ciphertext is not random data generated by a cryptographically secure pseudorandom number generator. This is used in combination with some decoy data that the user would plausibly want to keep confidential that will be revealed to the attacker, claiming that this is all there is. This form of deniable encryption is sometimes referred to as steganography. The user can supply any incorrect key for the truly secret data, which will result in apparently random data, indistinguishable from not having stored any particular data there.

One example of deniable encryption is a cryptographic filesystem that employs a concept of abstract "layers", where each layer would be decrypted with a different encryption key. Additionally, special "chaff layers" are filled with random data in order to have plausible deniability of the existence of real layers and their encryption keys. The user will store decoy files on one or more layers while denying the existence of others, claiming that the rest of space is taken up by chaff layers. Physically, these types of filesystems are typically stored in a single directory consisting of equal-length files with filenames that are either randomized (in case they belong to chaff layers), or cryptographic hashes of strings identifying the blocks. The timestamps of these files are always randomized. Examples of this approach include Rubberhose filesystem and PhoneBookFS.

Another approach utilized by some conventional disk encryption software suites is creating a second encrypted volume within a container volume. The container volume is first formatted by filling it with encrypted random data,[3] and then initializing a filesystem on it. The user then fills some of the filesystem with legitimate, but plausible-looking decoy files that the user would seem to have an incentive to hide. Next, a new encrypted volume (the hidden volume) is allocated within the free space of the container filesystem which will be used for data the user actually wants to hide. Since an adversary cannot differentiate between encrypted data and the random data used to initialize the outer volume, this inner volume is now undetectable. Concerns have, however, been raised for the level of plausible deniability in hiding information this way – the contents of the "outer" container filesystem (in particular the access or modification timestamps on the data stored) could raise suspicions as a result of being frozen in its initial state to prevent the user from corrupting the hidden volume. This problem can be eliminated by instructing the system not to protect the hidden volume, although this could result in lost data. FreeOTFE and BestCrypt can have many hidden volumes in a container; TrueCrypt is limited to one hidden volume.[4]

### Detection

The existence of a hidden volume may be revealed by flawed implementations relying on predictable cryptographic items[5] or by some forensic tools that may detect non-random encrypted data.[6][7] Vulnerability to chi-squared randomness test has also been suggested: encrypted data, after each write operation, should be adjusted to fit a plausible randomness property.[8]

Deniable encryption has also been criticized because of its main inability in defending users from rubber-hose cryptanalysis. Possession of deniable encryption tools could lead attackers to continue an investigation even after a user pretends to cooperate, providing an expendable password to some decoy data.[9]

## Malleable encryption

Some in-transit encrypted messaging suites, such as Off-the-Record Messaging, offer malleable encryption which gives the participants plausible deniability of their conversations. While malleable encryption is not technically "deniable encryption" in that its ciphertexts do not decrypt into multiple plaintexts, its deniability refers to the inability of an adversary to prove that the participants had a conversation or said anything in particular.

This is achieved by the fact that all information necessary to forge messages is appended to the encrypted messages – if an adversary is able to create digitally authentic messages in a conversation (see hash-based message authentication code (HMAC)), he is also able to forge messages in the conversation. This is used in conjunction with perfect forward secrecy to assure that the compromise of encryption keys of individual messages does not compromise additional conversations or messages.

## Software

- OpenPuff, freeware semi-open-source steganography for MS Windows.
- BestCrypt, commercial on-the-fly disk encryption for MS Windows.
- FreeOTFE, opensource on-the-fly disk encryption for MS Windows and PocketPC PDAs that provides both deniable encryption and plausible deniability.[10] Offers an extensive range of encryption options, and doesn't need to be installed before use.
- Off-the-Record Messaging, a cryptographic technique providing true deniability for instant messaging.
- PhoneBookFS [11], another cryptographic filesystem for Linux, providing plausible deniability through chaff and layers. A FUSE implementation. No longer maintained.
- rubberhose [12]. Defunct project (Last release in 2000, not compatible with modern Linux distributions)
- StegFS, the current successor to the ideas embodied by the Rubberhose and PhoneBookFS filesystems
- TrueCrypt, which is on-the-fly disk and folder encryption software for Windows, Mac and Linux that provides limited deniable encryption[13] and to some extent (due to limitations on the number of hidden volumes which can be created) plausible deniability, and doesn't need to be installed before use as long as the user has full administrator rights
- Vanish - a research prototype implementation of self-destructing data storage
- ScramDisk 4 Linux - A free software suite of tools, for GNU/Linux systems, which can open and create scramdisk and truecrypt container.

## References

[1] See http://www.schneier.com/paper-truecrypt-dfs.html.Retrieved on 2013-07-26.
[2] See http://iq.org/~proff/rubberhose.org/.Retrieved on 2009-07-22.
[3] http://www.freeotfe.org/docs/Main/plausible_deniability.htm
[4] http://www.truecrypt.org/hiddenvolume
[5] Encrypted hard drives may not be safe: Researchers find that encryption is not all it claims to be. (http://news.techworld.com/security/102171/encrypted-hard-drives-may-not-be-safe/)
[6] TrueCrypt is now Detectable (http://www.forensicinnovations.com/blog/?p=7)
[7] TCHunt, Search For TrueCrypt Volumes (http://www.ghacks.net/2011/04/11/tchunt-search-for-truecrypt-volumes/)
[8] MultiObfuscator - Manual: Architecture and chi-squared self-defense (http://embeddedsw.net/doc/MultiObfuscator_Help_EN.pdf)
[9] Julian Assange: Physical Coercion (http://embeddedsw.net/doc/physical_coercion.txt)
[10] See its documentation section on "Plausible Deniability" (http://www.freeotfe.org/docs/Main/plausible_deniability.htm))
[11] http://www.freenet.org.nz/phonebook/
[12] http://iq.org/~proff/rubberhose.org/
[13] TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software for Windows Vista/XP, Mac OS X, and Linux - Hidden Volume (http://www.truecrypt.org/hiddenvolume.php)

## Further reading


- Czeskis, A.; St. Hilaire, D. J.; Koscher, K.; Gribble, S. D.; Kohno, T.; Schneier, B. (2008). "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications" (http://www.usenix.org/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf). *3rd Workshop on Hot Topics in Security*. USENIX.
- Howlader, Jaydeep; Basu, Saikat (2009). "Sender-Side Public Key Deniable Encryption Scheme". *Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing*. IEEE. doi: 10.1109/ARTCom.2009.107 (http://dx.doi.org/10.1109/ARTCom.2009.107).
- Howlader, Jaydeep; Nair, Vivek; Basu, Saikat (2011). "Deniable Encryption in Replacement of Untappable Channel to Prevent Coercion". *Proc. Advances in Networks and Communications*. Communications in Computer and Information Science **132**. Springer. pp. 491–501. doi: 10.1007/978-3-642-17878-8_50 (http://dx.doi.org/10.1007/978-3-642-17878-8_50).

# Article Sources and Contributors

**Deniable encryption** *Source*: https://en.wikipedia.org/w/index.php?oldid=572932284 *Contributors*: Aalevy, Apokrif, Arkixml, Badger Drink, Bearcat, Bender235, Blackvisionit, Blammermap, Charles Matthews, Chrismiceli, Ciphergoth, Ciphers, CommonsDelinker, Cookiehead, Cralar, D. Wu, Dab Brill, David Haslam, Decrypt3, Dougher, Doyley, Eric.weigle, Fedkad, FireDemon, Frap, H8gaR, Harel, Hurricanefloyd, Iandiver, Ignorexxia, Ingolfson, Intgr, Jthill, Justin W Smith, Legoktm, Leobold1, LinuxAngel, MaxLanar, Maxt, Mìthrandir, Nabokov, Nikita Borisov, Nuwewsco, OMouse, Perey, Pol098, Raftermast, Richard506, Rjwilmsi, Ronark, Smb1001, Stevo2001, Stphnlee, Sverigekillen, Taejo, The Firewall, The Man Hole, Trakon, TreasuryTag, Urgos, Vanished user uih38riiw4hjlsd, Wavelength, Widefox, Wittylama, XFireRaidX, ZipoBibrok5x10^8, 88 anonymous edits

# License