Be A Hero: Encrypt Documents For Free In 3 Steps, And Learn Enough To Teach Your Clients And Opposing Counsel
(Learn Why Encryption Is Good Business And How It Works)

by Ronald L. Chichester[1]

1. Introduction

Encryption is the process of encoding information so that only the sender and the intended recipient can use that information.[2] Encryption is widely viewed as the single best security measure that one can take to secure digital information.[3] Indeed, all forty-seven states that have data breach/notification laws cite encryption as a valid mechanism ("safe harbor") to protect data and preclude the need to notify victims if the security of an information system is breached.[4] This paper will explain why attorneys need to encrypt information, what information

---

1 B.S. Aerospace Engineering 1982, University of Michigan; M.S. Aerospace Engineering 1984, University of Michigan; J.D. 1991, University of Houston Law Center. Past Chair of the Business Law and the Computer & Technology Sections of the State Bar of Texas. Registered Patent Attorney, Certified Computer Forensic Examiner and Certified Information Systems Auditor.

2 For the definition of encryption, *see, e.g.*, the Merrian Webster definition, available at: http://www.merriam-webster.com/dictionary/encrypt. *See generally*, BRUCE SCHNEIRER, APPLIED CRYPTOGRAPHY (2d ed., 1996).

3 *See, e.g.*, http://www.webopedia.com/TERM/E/encryption.html. *See generally,* BRUCE SHNEIRER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000).

4 *See*, Alaska Stat. § 45.48.010 et seq., Ariz. Rev. Stat. § 44-7501, Ark. Code § 4-110-101 et seq., Cal. Civ. Code §§ 1798.29, 1798.80 et seq., Colo. Rev. Stat. § 6-1-716, Conn. Gen Stat. § 36a-701b, 2015 S.B. 949, Public Act 15-142, Del. Code tit. 6, § 12B-101 et seq., Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) , Ga. Code §§ 10-1-910, -911, -912; § 46-5-214, Haw. Rev. Stat. § 487N-1 et seq., Idaho Stat. §§ 28-51-104 to -107, 815 ILCS §§ 530/1 to 530/25, Ind. Code §§ 4-1-11 et seq., 24-4.9 et seq., Iowa Code §§ 715C.1, 715C.2, Kan. Stat. § 50-7a01 et seq. , KRS § 365.732, KRS §§ 61.931 to 61.934 , La. Rev. Stat. §§ 51:3071 et seq., 40:1300.111 to .116 , Me. Rev. Stat. tit. 10 § 1347 et seq., Md. Code Com. Law §§ 14-3501 et seq., Md. State Govt. Code §§ 10-1301 to -1308, Mass. Gen. Laws § 93H-1 et seq., Mich. Comp. Laws §§ 445.63, 445.72, Minn. Stat. §§ 325E.61, 325E.64, Miss. Code § 75-24-29, Mo. Rev. Stat. § 407.1500, Mont. Code §§ 2-6-1501 to -1503, 30-14-1701 et seq., 33-19-321, Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807, Nev. Rev. Stat. §§ 603A.010 et seq., 242.183, N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21; 189:66, N.J. Stat. § 56:8-161, -163, N.Y. Gen. Bus. Law § 899-aa, N.Y. State Tech. Law 208, N.C. Gen. Stat §§ 75-61, 75-65, N.D. Cent. Code §§ 51-30-01 et seq., 51-59-34(4)(d), Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192, Okla. Stat. §§ 74-3113.1, 24-161 to -166, Oregon Rev. Stat. § 646A.600 to .628, 2015 S.B. 601, Chap. 357, 73 Pa. Stat. § 2301 et seq., R.I. Gen. Laws § 11-49.2-1 et seq., 2015 S.B. 134, Public Law 2015-138, 2015 H.B. 5220, Public Law 2015-148, S.C. Code § 39-1-90, 2013 H.B. 3248, Tenn. Code § 47-18-2107; § 8-4-119 (2015 S.B. 416, Chap. 42), Tex. Bus. & Com. Code §§ 521.002, 521.053; Tex. Ed. Code § 37.007(b)(5); Tex. Pen. Code § 33.02, Utah Code §§ 13-44-101 et seq.; § 53A-13-301(6), Vt. Stat. tit. 9 § 2430, 2435, Va. Code § 18.2-186.6, § 32.1-127.1:05, § 22.1-20.2, Wash. Rev. Code § 19.255.010, 42.56.590, 2015 H.B. 1078, W.V. Code §§ 46A-2A-101 et seq., Wis. Stat. § 134.98, Wyo. Stat. § 40-12-501 et seq., D.C. Code § 28- 3851 et seq., 9 GCA § 48-10 et seq., 10 Laws of Puerto

should be encrypted, and how to encrypt that information so that it may be shared with clients in a relatively safe manner.

2. Why Encrypt?

Twenty years ago, few attorneys encrypted their data. Today, with the widespread use of the Internet and the vast bulk of attorney work product and evidence being in digital form, most clients assume that an attorney should possesses the requisite competence to secure their confidences and privileged information with encryption technology. Indeed, the need for encryption is *more* acute for law firms than it is for clients because, unfortunately, law firms have become one of the primary avenues that hackers use for corporate espionage.[5] Business law firms are not the only ones targeted. Other targets include intellectual property firms (for corporate espionage and trade secret misappropriation), tax firms (identity theft), and family law firms (identity theft). Large law firms are attacked daily. Worse, the cost of hacking has plummeted in the last few years because of widespread availability of high-quality hacking code developed by the United States finding itself "in the wild."[6] This means that mid-sized law

Rico § 4051 et seq., V.I. Code tit. 14, § 2208

5 A classic case involves the PotashCorp, a company whose law firm was targeted to gain secrets regarding an acquisition. CBCNews, *Foreign Hackers Targeted Canadian Firm* (Nov. 30, 2011), *available at* http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810; BloombergBusiness, *China-Based Hackers Target Law Firms to Get Secret Data* (Jan. 31, 2012), *available at* http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms

6 Partial source code for the Stuxnet botnet virus is on multiple websites. Some of the sites charge a fee, some are for free. Support contracts are available at a modest fee. For example, a partial decompilation of the machine code to source code of the Stuxnet botnet virus is available at https://github.com/Laurelai/decompile-dump. The aforementioned virus is the "payload" of another (penetration) tool that is used to deliver the payload to a designated website, such as the one belonging to the law firm. Several very good penetration tools are available for free or modest cost on the Internet, such as Metasploit (http://metasploit.com/), Nessus (http://www.tenable.com/products/nessus-vulnerability-scanner), Netsparker (http://www.mavitunasecurity.com/netsparker/), and others. *See*, e.g., Software Testing Help, *37 Powerful Penetration Testing Tools For Every Penetration Tester* (Nov. 3, 2015) available at http://www.softwaretestinghelp.com/penetration-testing-tools/. In fact, some of the data needed to hack into law

firms, and even small law firms, are economically viable targets. Consequently, because all law firms are potential (and juicy) targets, getting hacked is foreseeable and so countermeasures, such as encryption, are necessary.

3. What to Encrypt?

Security is hard and insecurity is easy.[7] Safeguards are expensive, degrade efficiency, and are never foolproof. A proper security scheme has to accommodate a seemingly infinite variety of attacks, but the hacker only needs to be right once. Consequently, security is a never-ending allocation of risks -- a trade-off between expense and efficiency on one side, and the cost of compromise on the other. Striking the right balance is a difficult business choice.

Fortunately, not everything needs to be encrypted. Information that is available publicly rarely needs to be encrypted. However, the combination of information that is available publicly with other information (such as a bank account number) might constitute information that crosses a statutory threshold that commands additional protection.[8] Moreover, other types of information not related to bank accounts can constitute client confidences that require the attorney to protect accordingly pursuant to each state bar's disciplinary rules.[9]

---

firms may already be available via Google, whose cache service holds a bevy of information needed by hackers. *See, generally*, Johnny Long, *Google Hacking for Penetration Testers*, available at https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf (and Mr. Long has a full-length book by the same title that is available in many book stores, including Amazon.com).

7 *See, e.g.*, InfoWorld, *6 Reasons Why Security Is So Hard* (Mar. 16, 2015) available at http://www.infoworld.com/article/2896513/security/why-improving-security-is-so-hard.html; Ross Anderson, *Why Information Security Is Hard – An Economic Perspective*, available at https://www.acsac.org/2001/papers/110.pdf

8 See, supra, note 4.

9 *See*, Texas Disciplinary Rule 1.05 (hereinafter, TEX D.R. 1.05). Rule 1.05 states, in part: "(a) Confidential information includes both privileged information and unprivileged client information. Privileged information refers to the information of a client protected by the lawyer-client privilege of Rule 5.03 of the Texas Rules of Evidence or of Rule 5.03 of the Texas Rules of Criminal Evidence or by the principles of attorney-client

Moreover, data rarely needs to remain encrypted forever.[10] Security of the data is needed only so long as the *secrecy* of the data has value. Consequently, the cost of security can be mitigated if the conditions so allow. Standard document retention policies can apply regardless of whether the data is encrypted or not.

4. How to Encrypt?

Encryption schemes typically address two areas: the encryption of the *documents* themselves, or the encryption of the *transmission* of the unencrypted documents. This paper will address both types of schemes.

a. *Transmission Encryption*

Transmission encryption is often easier for the client. While document encryption may be desirable for the attorney, encryption may be a difficult encumbrance for individuals or small companies that do not have the steady flow of work that prompts adoption of document encryption. Transmission encryption typically entails the securing of the means to communicate between the lawyer's server and the client's device. There are two main ways to accomplish transmission encryption: secure web transaction and virtual private networks ("VPN"). Each option has pros and cons, but both need a digital certificate and both need specialized software.

privilege governed by Rule 5.01 of the Federal Rules of Evidence for United States Courts and Magistrates. Unprivileged client information means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client. (b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e), and (f), a lawyer shall not knowingly: (1) Reveal confidential information of a client or a former client to: (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the clients representatives, or the members, associates, or employees of the lawyers law firm."

10 Note, however, that in some states such as Texas, encrypting an electronic document is considered (statutorily) equivalent to its destruction. *See, e.g.*, TEX. BUS. & COMM. CODE 521.052(b)(3) ("otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means"), which can include encryption and purposefully losing the key(s).

i. Digital Certificate

Because the design of the Internet makes it difficult to know if a someone on the other end is who they say they are, computer scientists and security professionals devised a mechanism to use third parties to vouch for organizations. That "voucher" is in the form of a digital certificate, and is used by web browsers and VPN clients to establish an encrypted conversation.

Digital certificates are issued by an organization called a certification authority. The certification authority is a third party that vouches for the authenticity of a server operating with the law firm's domain name (e.g., bakerbotts.com). Normally, the law firm enters into an arrangement with a certification authority (for a fee). Once the firm's application has been approved, the certification authority issues the digital certificate to certify (to the client's software) the authenticity of the encryption key that is used to establish an encrypted communication between the law firm and the client. For the law firm, there are several certification authorities from which to choose. Not all digital certificates are expensive however. The *Let's Encrypt* project provides digital certificates in an automated (and thus extremely low cost) fashion.[11]

ii. *Secure Hyper Text Transfer Protocol (https) Web Server*

The first way to secure communications is for the lawyer to employ a secure web server (e.g., one using http**s** rather than simple http). One nice feature about this approach is that the law firm can accomplish the setup automatically, with minimal fuss for the client. Moreover, the client only needs to enter the law firm's domain name on most any standard web browser, further

11 Information about the free digital certificates, which can be generated freely and automatically, can be found at https://letsencrypt.org/. That project has the backing of major Internet companies and organizations.

facilitating the setup. Fortunately, there are software solutions for secure web transactions that are available for free. For example, the open source Apache web server is perfectly capable of conducting secure web transmissions.[12] If an attorney has a web server, chances are that minor changes to the web server's settings can enable secure transactions. Many Internet Service Providers enable connectivity for a modest fee (or for no additional fee). Note, in order to avoid some disturbing error messages on the client's side, a working digital certificate is necessary. Secure web servers are particularly useful when the client is entering

iii. Virtual Private Network

The second common way to secure communications is to erect a virtual private network ("VPN") between the lawyer firm's network and the client's device. VPN's are most useful when the lawyer and client transfer large amounts of information on a regular basis, such as when the client needs to upload large numbers of documents for litigation. A VPN requires specialized software on both the law firm's side and the client's side to handle the encryption and decryption. The Internet is simply used as a common connection mechanism to facilitate the transfer of bits between the client and the law firm. Since all of the software on either end encrypts all traffic going over the Internet, transmission of client data can be made in confidence. Normally, a special server (called a Network Access Server or "NAS") is connected to the law firm's network. NAS's are not particularly high-powered machines. Indeed, former desktop PC's are often pressed into service as a low-cost NAS. However, because the NAS must be exposed to the Internet, it is vital that the specific configuration settings are made competently, lest the NAS

12 Complete instructions for conducted secure (encrypted) web transactions can be found at https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html

be the source of a data breach of the law firm's network. Open source software is available for the NAS to handle the VNP transactions on the law firm's side to so costs can be contained.[13] So long as standard communication protocols are employed, the lawyer's clients will have a range of choices for the specialized software on their side that could interoperate with the law firm's VPN.[14]

b. *Document Encryption*

Document encryption is the best single option that an attorney can elect to protect client confidences and take advantage of safe harbor provisions afforded by many states.[15] Secondly, transmitting client information in the form of an encrypted attachment to an email obviates the need for a secure website or a VPN. Third, the client has the option to store the information in encrypted form, which may afford the client the same safe harbor provisions as the attorney. Documents transmitted via a VPN or secure web server are ***not*** considered encrypted and thus do not come under the safe harbor provisions.

As with transmission encryption, there are many options available for attorneys to encrypt documents. The number of options expands *if* the clients only receive their information in unencrypted form. However, if clients opt for receiving the attorney work product in encrypted form, then there are additional considerations for the attorney.

Exchanging encrypted documents requires that both sides agree on certain technical

13 The software to create a VPN server can be found at https://openvpn.net/, and client versions for that VPN system are available for Windows, Mac OS X, iOS, Android and Linux at that same website.

14 *See, e.g.*, LifeHacker, *Five Best VPN Tools* (Mar. 7, 2010) available at http://lifehacker.com/5487500/five-best-vpn-tools.

15 *See*, *supra*, note 4.

requirements, namely: common encryption algorithm, common file format, and common (or coordinated) keys. Lack of coordination often means that the data is unusable by one side or the other. However, adequate coordination is usually achieved easily by simply using the same software application on both sides.

i. *Encryption Algorithm*

You cannot encrypt a file in a random manner. In order to decrypt a file (and thus use the information later) you need to be able to reverse the encryption process *precisely*. There are a variety of encryption algorithms in widespread use, including AES, RSA, and DES.[16] So the first choice in the development of a secure communication mechanism between the attorney and the client is the adoption of a common encryption algorithm.

ii. *File Format*

Even though two different encryption software applications use the same encryption algorithm, they may not store the resulting encrypted document in the same format. Unfortunately, there is no common convention in the formatting of encrypted documents. Consequently, before decryption can take place, the software application has to be able to interpret the document properly in order to decrypt it correctly. The practical effect of this dilemma is to encourage both client and lawyer to use the same encryption software application.

iii. *Keys*

All encryption algorithms employ one or more keys in the encryption and decryption process. Keys are composed of bits. The more bits in the key, the harder it is to break by trying

16 *See*, *generally*, Gurpreet Singh and Supriya, *A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security*, International Journal of Computer Applications, Vol. 67, No. 19 (April, 2003) available at http://research.ijcaonline.org/volume67/number19/pxc3887224.pdf

all possible combinations (*i.e.*, "brute force"). Rhode Island was the first state to establish a bit-length needed to come under its safe harbor provision, and that length is 128 bits. Incidentally, 128 bits is the standard key length for financial transactions (e.g. e-commerce purchases) over the Internet. Most decent encryption software programs currently use a 256-bit key length, and that is what I recommend to my clients.

iv. *Passwords*

A chain is only as strong as its weakest link. The best encryption algorithms are rendered moot when the users adopt short, easy or common passwords. There are strong password generators available for free.[17] Unfortunately, strong passwords are often hard to remember, which prompts the use of a password manager, or at the least some type of password convention. There are several good password managers available, most for free or for a modest fee.[18]

iv. *Choice of Software*

To eliminate format and algorithm mismatches, lawyers often opt to use a software application that their client employs. Large corporations probably already have a preferred application, and the lawyer is expected to adopt it. For small or mid-sized firms, however, the lawyer is often in the position to recommend something. It has been my experience that small companies or individuals will use something that doesn't cost them any money, and is easy to use. Secondly, the encryption software must be cross-platform, because many lawyers prefer Macs, clients tend to be stuck on Windows, and sophisticated attorneys and clients opt for Linux. Finally, the encryption software needs to be available for long periods of time, so the license

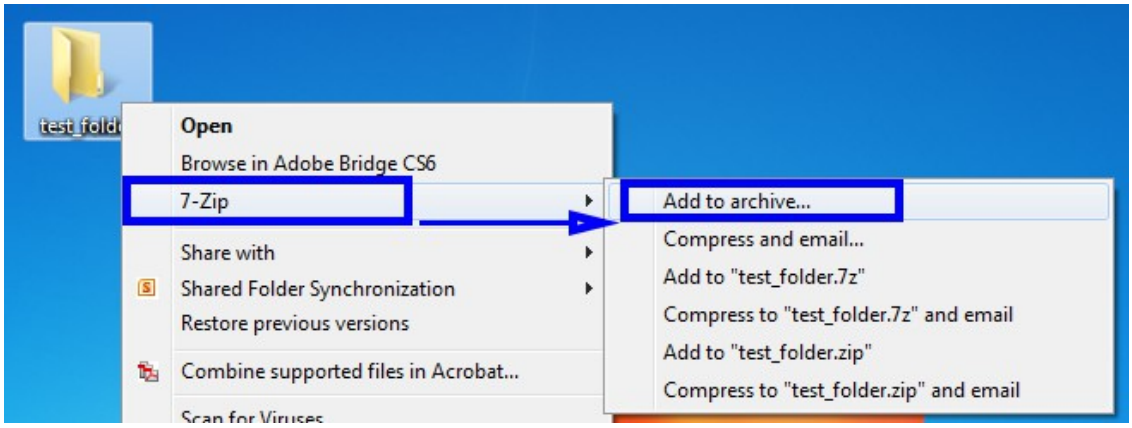
17 One example of a free secure password generator is available at http://passwordsgenerator.net/

18 LifeHacker, *Five Best Password Managers* (Jan. 11, 2015) available at http://lifehacker.com/5529133/five-best-password-managers.

agreement for the software must allow for having older versions of the software available to eliminate compatibility problems. Finally, the software needs to be easy to use – because you want to make it easy for all involved to do the right thing.

Fortunately, there are several encryption software applications that satisfy all of the aforementioned requirements. Two applications in particular have merit. The first application is called 7zip.[19] The second application is called AESCrypt.[20]

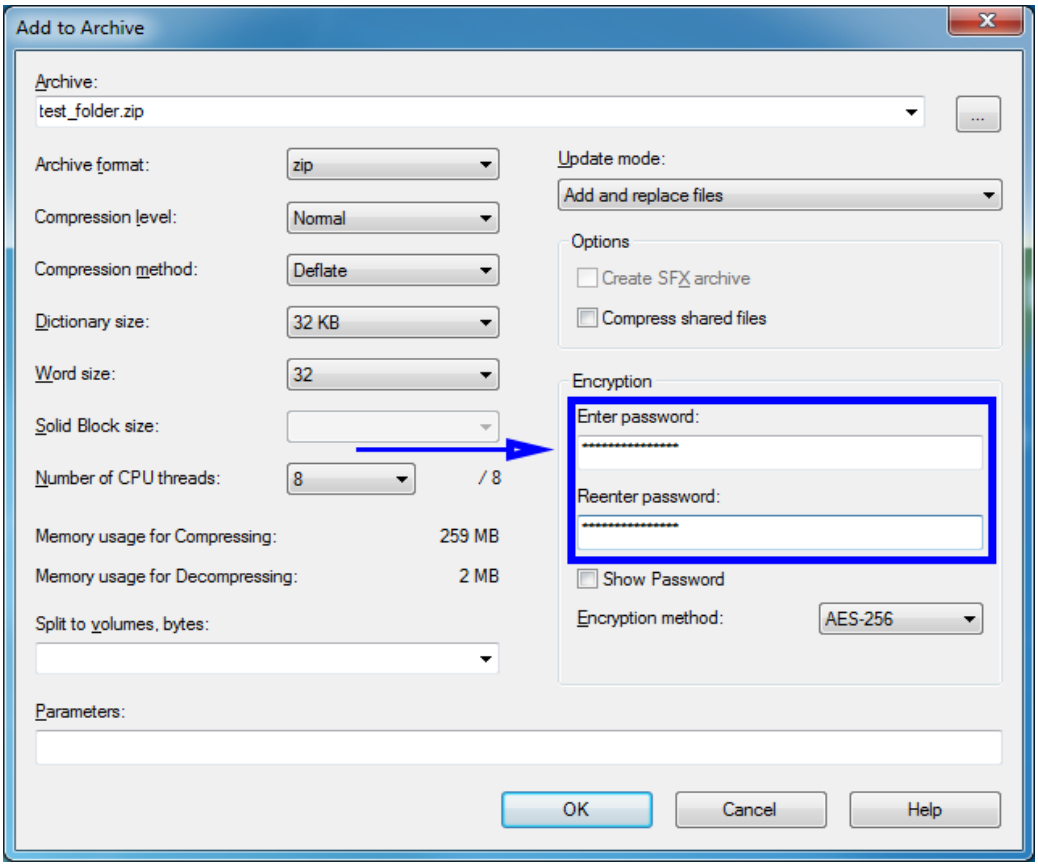
7zip, as the name implies, is primarily a file compression tool. However, it has a handy encryption feature that provides 256-bit AES encryption capability that is easily invoked. For example, to encrypt a file (or folder), merely right-click on it as shown below.



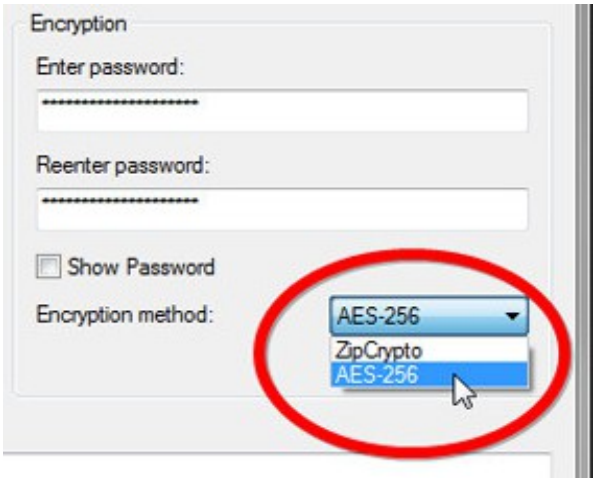
You can create a new archive, or add the file(s)/folder(s) to an existing archive. If you add it to an existing archive, a dialog box will appear and you will be given the opportunity to encrypt the archive as shown below.

19 7zip is available at http://www.7-zip.org/. 7zip is an open source application that can compress and encrypt individual files, sets of file, or entire folders. Binary executables are available on that website for all flavors of Windows, Mac OSX and Linux.

20 AESCrypt is available at https://www.aescrypt.com/. AESCrypt is an open source application that works on Windows, Mac OSX and Linux.



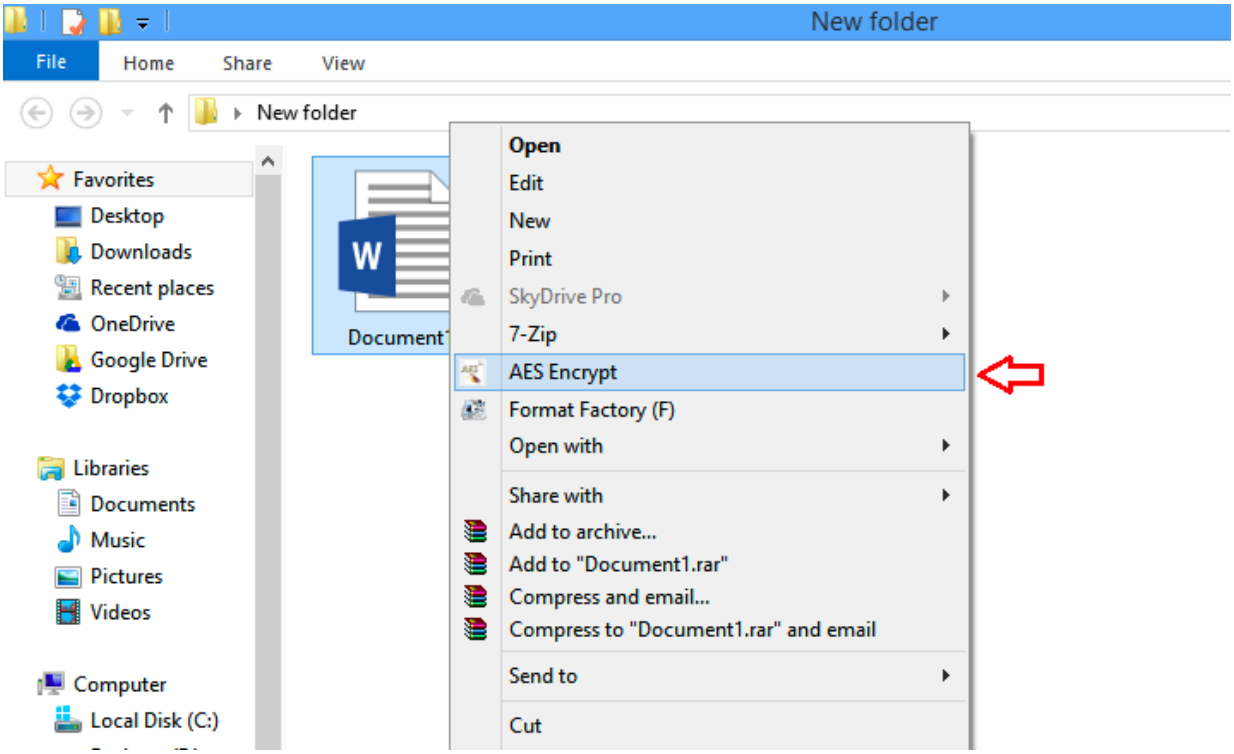
Note, the "Encryption method" (below the blue box) is set to AES-256, meaning that the algorithm used is AES, and the key length is 256 bits. 7zip has a choice of two encryption algorithms (as shown below), but AES-256 is the one recommended by the author.



AESCrypt

AESCrypt is an open source application that is designed specifically (and solely) for encryption. It was originally designed to generate an encrypted copy of an electronic file so that it may be attached to an email message. The advantage of AESCrypt is that, once set up, it is very easy to use. Upon setup, an icon will be placed on the desktop (or dock).

To invoke the program, all that you need to do is drag the file to the desktop icon. Alternatively, you can highlight the file, right-click and select "AES Encrypt" as shown below.



The program will prompt you for the password. Enter the password, and you're done. Simple. Incidentally, the same process works for encryption and decryption. To decrypt an encrypted document, simply perform the same steps. Right-click or drag-and-drop the file to the AESCrypt icon. The program is smart enough to know what to do.

One downside to AESCrypt is that it deals only with one file at a time. You cannot select groups of files or folders for encryption. The simplest work-around to this limitation is that you can create a zip archive using standard tools, and then encrypt that zip file. Since AESCrypt makes an encrypted *copy* of the file, you have to delete the unencrypted version in order to be safe. From a security standpoint, however, encrypting ever single document (individually, each with its own password), is best from a security standpoint.

A bonus feature of AESCrypt is that there are versions written in Java and PHP so websites can, for example, be retrofitted to encrypt documents that are uploaded to the firm's server by clients.

5. Conclusions

The need for encryption is immediate and real. Texas law and disciplinary rules incentivize lawyers to encrypt their client's data. Attorneys have a bounty of options for encrypting documents and transactions with clients. Low-cost options are available to implement an encryption scheme that benefits clients and provides protections for the lawyer. Moreover, because several of these options are open source software applications, they can be given to clients freely, thereby minimizing the cost to the client.