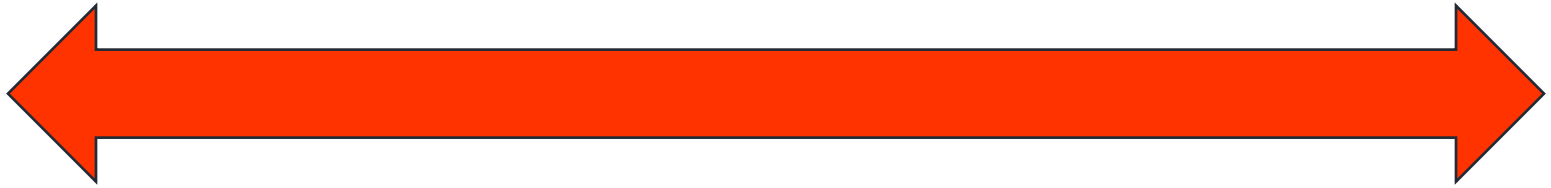
ENCRYPTION IS NOW CHEAP AND SIMPLE – AND MAY BE ETHICALLY REQUIRED!

D.C. Bar Association **May 6, 2016**

Sharon D. Nelson, Esq. & John W. Simek
snelson@senseient.com; jsimek@senseient.com

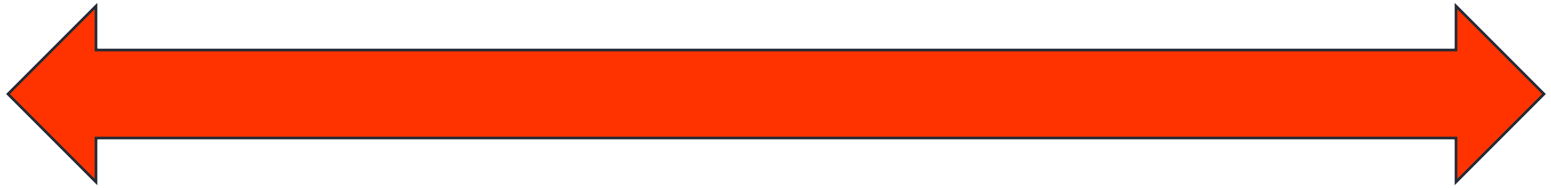
SENSEI ENTERPRISES 703.359.0700 WWW.SENSEIENT.COM

Is Encryption Ethically Required?



No Maybe Probably Definitely

Is Encryption Ethically Required?



Never **Sometimes** **Always**

Is Encryption Ethically Required?

"The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue [ethics] opinions suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required."
ABA, *Eye on Ethics* (July 2015)

YOUR ABA
e-news for members

Home > Publications > YourABA > 2015 > July 2015 > Encryption conniption

Encryption conniption

July 2015 | Eye on Ethics

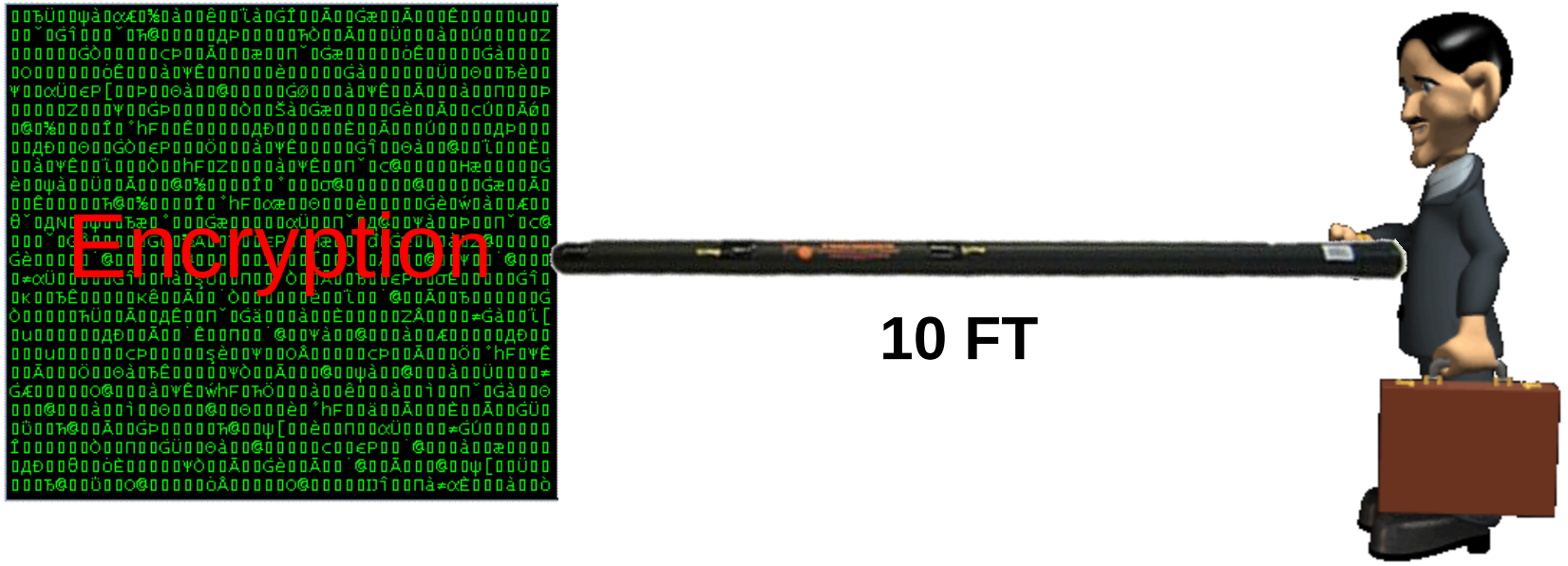
by
Peter Geraghty, director, ETHICSearch; and, Susan Michmerhuizen, ETHICSearch counsel, ABA Center for Professional Responsibility

Lost and Stolen Devices:

"Considering the high frequency of lost assets, encryption is as close to a no-brainer solution as it gets for this incident pattern. Sure, the asset is still missing, but at least it will save a lot of worry, embarrassment, and potential lawsuits by simply being able to say the information within it was protected."

"Competent and Reasonable Efforts"

Attorneys Avoid Encryption



ThinkGeek
STUFF FOR SMART MASSES

find stuff GO

FREE SHIPPING
ON ANY ORDER $75+
US Economy Only • No Code Needed
*Does not combine with other offers

Account | Wish Lists | Geek Points
Live Chat | Help
Have an account? Log In
Loot: Your cart is lonely

SHOP BY CATEGORY | SHOP BY INTEREST | MOTHER'S DAY | NEW | BESTSELLERS | EXCLUSIVES | T-SHIRTS | GADGETS | SALE

- Mother's Day
- Graduation Celebration
- T-Shirts & Apparel
- Geek Toys
- Electronics & Gadgets
- Home & Office
- Tools, Outdoor & Survival
- Geek Kids

Clearance SALE
Gift Certificates

Sign up for geek-mail
Your Email
RSS feeds

Home > Interests > Amazing Goodies >

Rosetta Stone® - Learn to Speak Klingon

©ThinkGeek.com
Click to zoom

Let language expand your universe!

- Learn to speak Klingon today
- Live conversation sessions with native speakers
- Free, downloadable mobile companion app
- Read more...

$269.99 ✓ Qapla'

Quantity: 1

BUY NOW or add to wish list

Like Share 25k | Tweet 296 | Pin it 71 | +1 462

Main Description | Additional Images

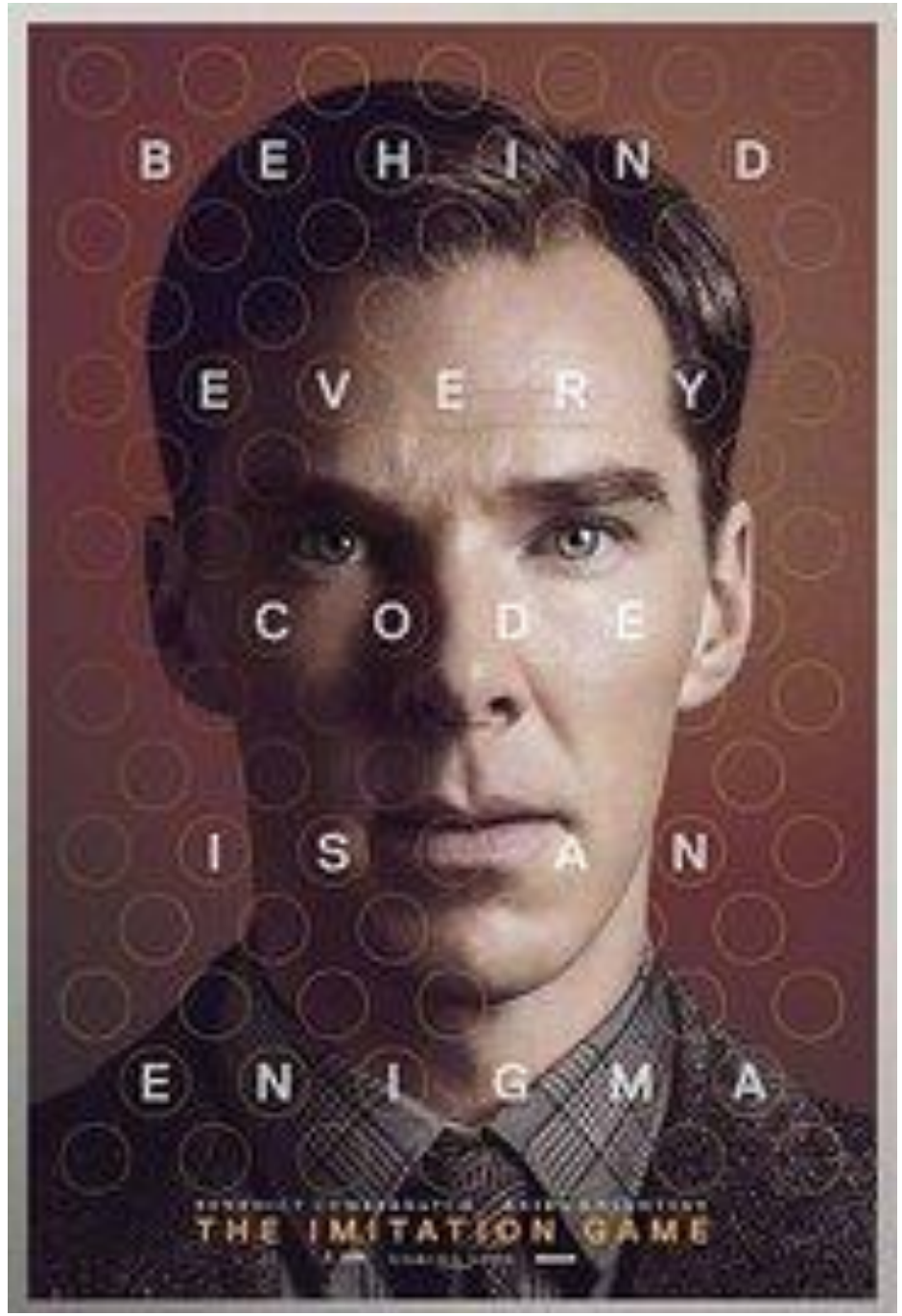
Customer Action Shots:

Watch the Video:

Your Fellow Smart Masses Also Bought:

Mr. Beard® Beard Machine

Unicorn Drinking Horn


BEHIND
EVERY
CODE
IS AN
ENIGMA
THE IMITATION GAME

Attorneys Avoid Encryption

- Encryption is too difficult.
- Encryption is too expensive.
- “I don’t need encryption!”

Why Attorneys Need Encryption

- Up to 70% of data breaches involve laptops & portable media.
- About 10% of laptops are stolen during their useful lives.
- 1.4 million smartphones were lost during 2013.
- 3.1 million smartphones were stolen during 2013.

Why Attorneys Need Encryption

- 8/11 Baltimore law firm
  (external hard drive – backup – left on light rail)
- 8/14 Law firm with GA operations center
  (external hard drive – backup - stolen from employee's trunk)
- 1/15 San Francisco attorney
  (laptop stolen)
- 4/15 San Diego law firm
  (laptop stolen on trolley)

Why Attorneys Need Encryption

- 2007: 18 laptops were stolen from the offices of a law firm in Orlando.
  - Protected by encryption
  - SANS Institute:
  "(laptop stolen, but the data was protected) shouldn't be newsworthy..."

Encryption protects data!

Why Attorneys Need Encryption

- Electronic communications can be intercepted.
- Wired and wireless network traffic can be intercepted.
- Cyberspace is a dangerous place!

Why Attorneys Need Encryption

Why Attorneys Need Encryption

PRISM

- **Web-based e-mail**
- **Telephone records**
- **Text messages**
- **Social media sites**
- **ISP communications**
- **VoIP**
- **File transfer**
- **Video conferencing**

Why Attorneys Need Encryption

TECHNOLOGY

242 COMMENTS

Security Experts Oppose Government Access to Encrypted Communication

By NICOLE PERLROTH JULY 7, 2015

Email

Share

Tweet

Save

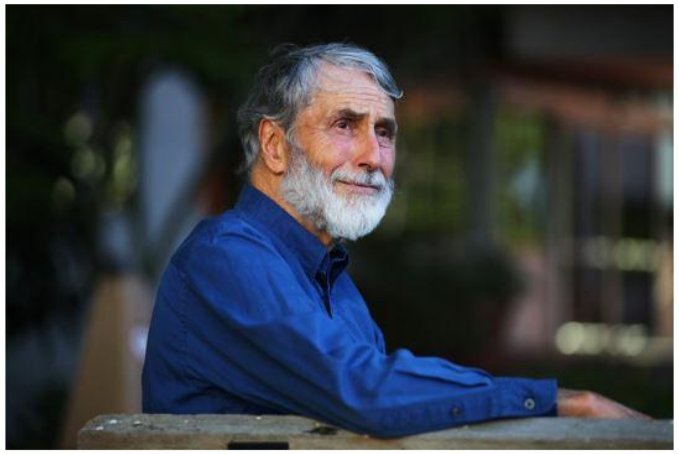
More

HE NAMED ME MALALA

SAN FRANCISCO — An elite group of security technologists has concluded that the American and British governments cannot demand special access to encrypted communications without putting the world's most confidential data and critical infrastructure in danger.

A new paper from the group, made up of 14 of the world's pre-eminent cryptographers and computer scientists, is a formidable salvo in a skirmish between intelligence and law enforcement leaders, and technologists and privacy advocates. After Edward J. Snowden's revelations — with security breaches and awareness of nation-state surveillance at a record high and data moving online at breakneck speeds — encryption has emerged as a major issue in the debate over privacy rights.

That has put Silicon Valley at the center of a tug



Peter G. Neumann, a computer security pioneer, says "there are more vulnerabilities than ever" that could be exploited through access to encrypted communications.
Jim Wilson/The New York Times

The 2015-16 Encryption Wars

The New York Times
July 7, 2015

FBI vs. Apple

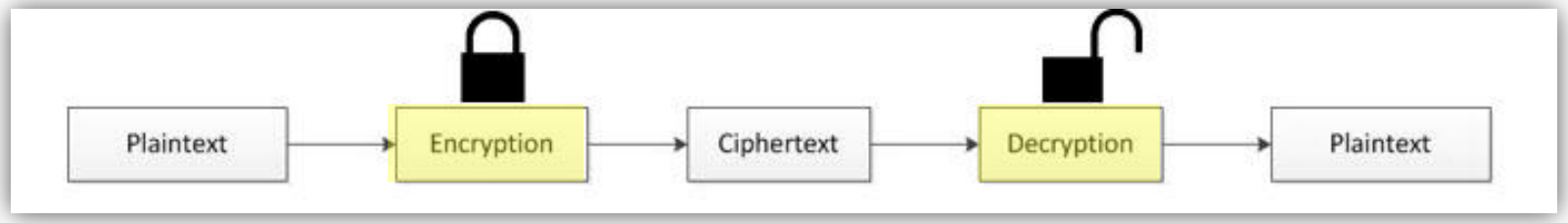
- iPhone 5c
- iOS 9
- PIN
- Backdoor

Encryption

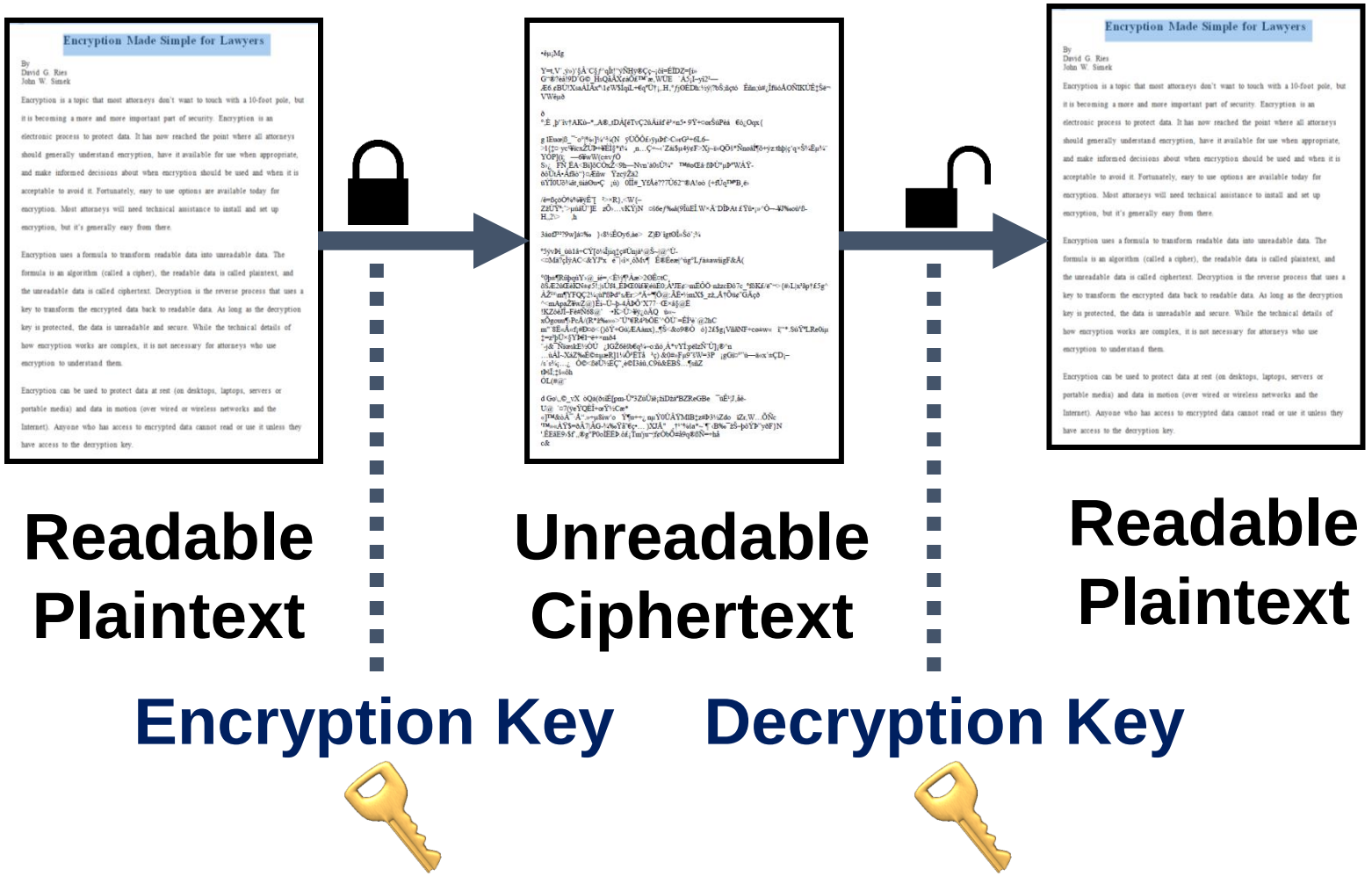
=An electronic process to protect data

=Transforms readable data into unreadable data

Requires a key to make data readable again



Encryption


Encryption Made Simple for Lawyers
By
David G. Ries
John W. Simek
Encryption is a topic that most attorneys don't want to touch with a 10-foot pole, but it is becoming a more and more important part of security. Encryption is an electronic process to protect data. It has now reached the point where all attorneys should generally understand encryption, have it available for use when appropriate, and make informed decisions about when encryption should be used and when it is acceptable to avoid it. Fortunately, easy to use options are available today for encryption. Most attorneys will need technical assistance to install and set up encryption, but it's generally easy from there.
Encryption uses a formula to transform readable data into unreadable data. The formula is an algorithm (called a cipher), the readable data is called plaintext, and the unreadable data is called ciphertext. Decryption is the reverse process that uses a key to transform the encrypted data back to readable data. As long as the decryption key is protected, the data is unreadable and secure. While the technical details of how encryption works are complex, it is not necessary for attorneys who use encryption to understand them.
Encryption can be used to protect data at rest (on desktops, laptops, servers or portable media) and data in motion (over wired or wireless networks and the Internet). Anyone who has access to encrypted data cannot read or use it unless they have access to the decryption key.
Readable Plaintext
Unreadable Ciphertext
Encryption Made Simple for Lawyers
By
David G. Ries
John W. Simek
Encryption is a topic that most attorneys don't want to touch with a 10-foot pole, but it is becoming a more and more important part of security. Encryption is an electronic process to protect data. It has now reached the point where all attorneys should generally understand encryption, have it available for use when appropriate, and make informed decisions about when encryption should be used and when it is acceptable to avoid it. Fortunately, easy to use options are available today for encryption. Most attorneys will need technical assistance to install and set up encryption, but it's generally easy from there.
Encryption uses a formula to transform readable data into unreadable data. The formula is an algorithm (called a cipher), the readable data is called plaintext, and the unreadable data is called ciphertext. Decryption is the reverse process that uses a key to transform the encrypted data back to readable data. As long as the decryption key is protected, the data is unreadable and secure. While the technical details of how encryption works are complex, it is not necessary for attorneys who use encryption to understand them.
Encryption can be used to protect data at rest (on desktops, laptops, servers or portable media) and data in motion (over wired or wireless networks and the Internet). Anyone who has access to encrypted data cannot read or use it unless they have access to the decryption key.
Readable Plaintext
Encryption Key
Decryption Key

•êµ¡Mg

Y=t,V´,ý»)‘§Â¨C§ƒ^qÎt!“ýÑHÿ®Çç~¡ôî=ÉÏDZ=[í»
G“®?èâ!9D´G©_HsQåÃX¢àÕ£™˜æ,WÜE `À5¡I–yî2²—
Æ6.¢BÙ!XsaÀÌÃx°\1¢W$ÍqiL+€q°Ü†¡,.H,°ƒjØÈDh:½ý|?bŠ;ñçtó Êñn;ù#¿ÎfüóÅOÑIKÚÊ‡Šë¬
VWêµð

ð
°;È ,þ′´îv†AKù–*„A®„tDÀ[êTvÇ2ûÄiâf ê³×n5• 9Ÿ+¤ørŠúPèá €ó¿Oqx{

g lEuœ|ß_ ¯¨o°|%‹]¼^¾(N ÿÙÕÔ£›ÿµÞf>C»rG³+6L6–
>1{‡¤·yc¹¥ïcxŽÙÞ+¥ÉÌ§*ï¾ ‚n…Ç÷~‹’Záı$µ4ÿ¢F>Xj~ï»QÕš*Ñnøâĺ¶õ+ýz:thþ|ç‘q×Š¾Ëµ¾¨
YÓP](ï¸ —6¥wW(c±vƒÖ
S›¿ FÑ¸ËA<Bi]õCÒxŽ<9h—Nvn’à0sÛ¾" ™#øŒâ·ßÞÙ°µÞ°WÁŸ-
ðôÛtÄ•Äfãò“}¤Æñw ŸzcÿŽã2
üÝÏ0Uõ¾ât¸üìàØu•Ç ¡ù) 0ÎÎ#_YfÅè???Û62“®A!øò {+fÚq™ᴮB¸ë›

/ê=ßçöÒ%%¥ÿÊ˜[²>×R},<W{–
ZžÙŸª;^>µúâÙ’]E zÕ›…vKÝjN ¤š6eƒ‰â(9ÎùEÎ.W×Ä¨DÎÞAt £Ÿû•¡»^Ò—¥J‰où¹ß-
H„2\> ‚h

3áøfJ³²?9w]á¤‰ }‹8½ÊOy6,àe> Z)Ð`îgtØÎ»Šó’;¾

°5ývÞî_ùù1â÷CÝ[õ¼Îjiq‡ç#Ùnjà¹@Š~|@^Ù-
<¤Mä?çÏÿAC<&YJ°x é¯|‹î×,ôMv¶ Ê®Éeæ|^úg°Lƒà±awîígF&Å(

Encryption Key

Example
AES-256 Key

+30NbBBMy7+1BumpfmN8QPHrwQr36/vBvaFLgQM561Q=

Encryption Key

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: BCPG C# v1.6.1.0

lQOsBFIOnHgBCACwAhCyBG5X52IkbIKpeN21wEa3kR+eLvqRkdjD1oL1o4kmy3hh
Zz1l/DH7RcZX+efCP3RfEvi7Mu3a9KIEq0D0KxLQbhaWvVDzJ8yUCR8kRepFDKtj
pj1G/049DJGM4AYHqhmTPSnwRnPBtv5Ci2k9cWgZSnH/4NnkAGYudsftReoxOsUt
pfYTyMeoGBg2DkNG4yZ6uG86v5k641lgH9qABajjFfXoe2aMwbYPMWQDahJlCZfH
U2q05GJt/2zThnky/D//savhrshpNxr1ddEa1QwgGSR/EDPkflv1b4yWH05DbRST
dR9B136kh+2YMDtqaJ75hhU/H9Q6WmhBAIlXABEBAAH/AwMCoZz7ekYu0YZgXUo
d
EoYlOwJmlu/ZLx2GSFtZO2RNyvblG+O3ZeKukG1xbSvzBS0Z5OjQOYnD+X5arvNM
DmpyilKpb5DueaN1osxPOkunqQ6cJlOWdROvUQkgLCD7Y7jfu4/coeK+HZuoIHSq
txEQaICTDcEnFYjDJNYNGWKj6WfT3LGjDhCreck6MZcGGJHjmCN8VF+yEmsUIkM+
9D/US/rl/lWnINlfgmhiN1NxpAhg9Xo43Mpwex3hZLXLrbhdTkRMVgHLEH5h3xxo
/UyNGCn3T9CTa4/vNdmZmMlAAHQk6F0ZhqFLS8x3sR2hxwkaNGmGHRr/ihklv15U
RrggHzH89zxc3RDC8al/wcieM1vXx9hK195r9NPJ/hET1EIqs3wLu8rmZDPazIVT
j8bQdhH3X964Q70ciiREVXbY29uwSXKHU6Q8agmCDdeGoZ/bhtLaYSs6Q53dgW97
U2IN6QIxHDTa+eZU5t1RVR5ugHph6yhTk6rCQF+FTsiaezwHkXqS5SfyNJ2JgOCi
6l4HpA2gLOy3raV4MoSpsEwIpquTccu/B8Aiucy6UL7IELOAMT2s7c2R7qVoBvew
5e2gDid0CWNqN03Zvg4USKq3lYskMUWUtaaexDWNALB210OKixm6mGN4VzelmqMK
w6drwWbfuo+Xt540wlGOOuCjZoEM+qxKofnDZicDQ9Lns/eswvLZS2L/ei3kF4du
B0wexeG7R5eNlOlDfReyz5qWXOLgS47In6OLBXlUfuuNsI0m64DM3Z9LBXev2TuG
YHGG26j1FRwgOdSDynjITA2xZrIJQ7rBjJhiMedH1bLlUau75EU/qQVAV1jZ+qD/
CbD/vxVW237NaAPPlctGXrvWMyZh/PSjb/wC56veYrQAiQEcBBABAgAGBQJSDpx4
AAoJEKJQRE9Opr2dRb8H/A67kPkY8fwCY8JxF6tV46rmXIyPOsVzVHb+TG9p+0ep
1js13t1MGJuMS7CXaDdtPdahD9IKwKRO3z2Jxsg2ADYditkR7QUknGUnrJsQOkKx
8gXinRihRNjM2JzsqWkBEOauIlnO5+Y01g7KTo93N1F+pNrPNzRko8gAPWIozJMd
5wLT9NvtdJLRumJjTjQ9ydyLa41uOq8EZvYELwyq0USO5AzlOu5XAduduRv9qhIm
CmN8RLgShJzCGhu2E08hgU2kZZtY1g3VyGnttkkn4Vtr6wREh5SyvMlzirWAMb1G
LvaFZWAYAPLlCtCZQU3pL8mjFTFAxsKS1CcRLUrOkLM=
=9Ry2

-----END PGP PRIVATE KEY BLOCK-----

A Simplified Overview

Encryption Program

Algorithm

Key

Protect

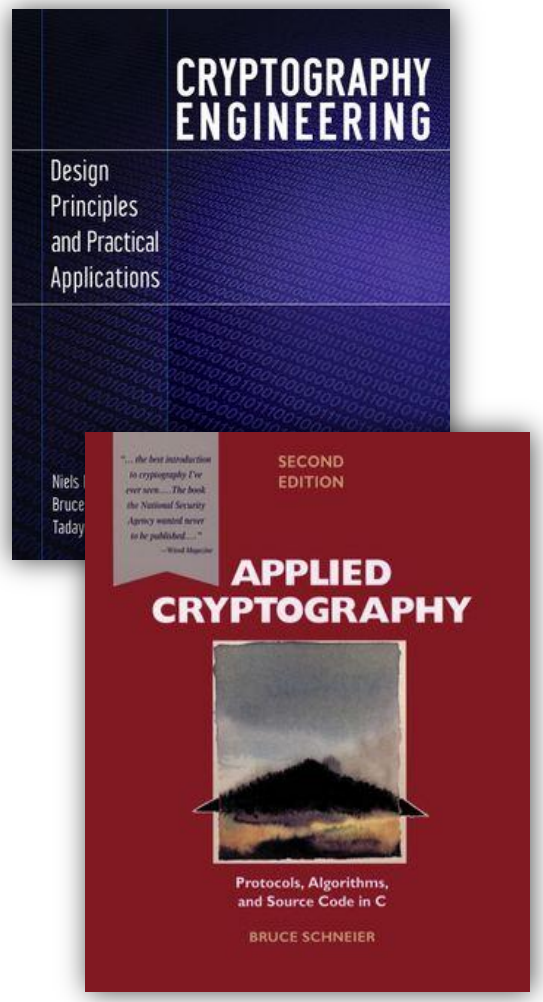
Data at Rest

- Servers, Desktops, Laptops, Tablets, Portable Media, Smartphones, etc.

Data in Motion

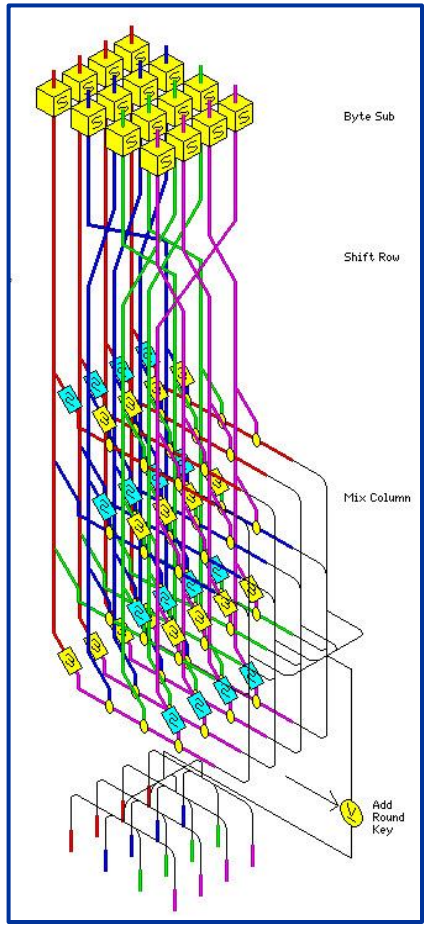
- Wired Networks, Wireless Networks, Internet, Cell Networks, etc.

Is Encryption Too Difficult?



AES ALGORITHM

Source: quadibloc.com



Is Encryption Too Difficult?

Attorneys will often need assistance in setting up encryption.

There are now many easy to use options for encryption (particularly after setup).

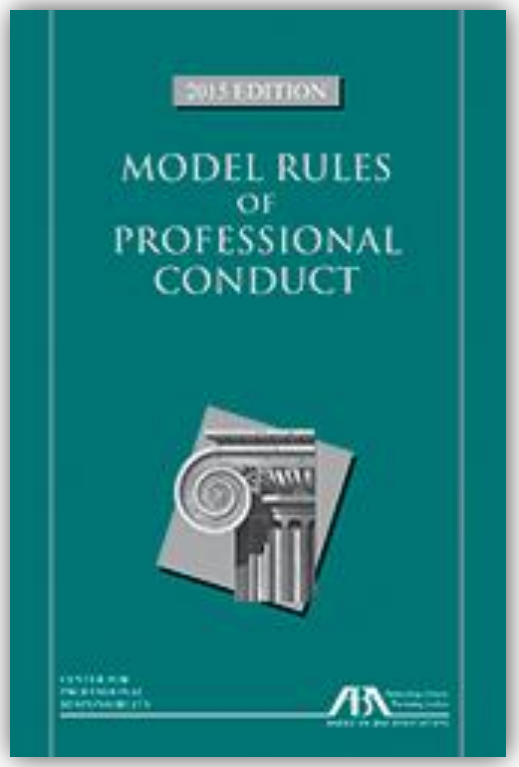
Attorneys' Duty to Safeguard

Ethics Rules

Common Law

Contracts

Statutes and Regulations



ABA Ethics 20/20 Amendments

Model Rule 1.1 Competence

Comment

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, <u>including the benefits and risks associated with relevant technology…</u>”

ABA Ethics 20/20 Amendments

Model Rule 1.6 Confidentiality

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

+ Comments 18 & 19

Ethics Opinions - Encryption

New Jersey Opinion 701 (2006)

California Formal Opinion No. 2010-179

Pennsylvania Formal Opinion 2011-200

Texas Opinion No. 648 (2015)

Unencrypted Email = “A Postcard”

"The common metaphor for Internet e-mail is postcards: Anyone – letter carriers, mail sorters, nosy delivery truck drivers - who can touch the postcard can read what's on the back."
Bruce Schneier 1995

“Reasonable Expectation of Privacy?”

Unencrypted Email = “A Postcard”

Email – A Postcard Written in Pencil

Larry Rogers 2001

SEI - Carnegie Mellon University

“Reasonable Expectation of Privacy?”

Unencrypted Email = "A Postcard"

"Emails that are encrypted as they're routed from sender to receiver are like sealed envelopes, and less vulnerable to snooping—whether by bad actors or through government surveillance—than postcards."
***Google Official Blog* June 2014**

"Reasonable Expectation of Privacy?"

Unencrypted Email = “A Postcard”

"Security experts say email is a lot more like a postcard than a letter inside an envelope, and almost anyone can read it while the note is in transit.”
***New York Times* July 2014**

“Reasonable Expectation of Privacy?”

Bottom Line

Encryption is increasingly required in areas like banking and health care and by new state data protection laws.

As these requirements continue to increase, it will become more and more difficult for attorneys to justify avoidance of encryption.

It has now reached the point where all attorneys should generally understand encryption, have it available for use when appropriate, and make informed decisions about when encryption should be used and when it is acceptable to avoid it.

Protect Decryption Key!

Generally requires password/passphrase to access key.

Use a strong password/phrase
- 14 characters or more.

Use a password manager for multiple encryption instances.

Passphrases

Iluvmy2005BMW!

IluvmXy2005B3MW!

<u>Stronger</u>: Break dictionary words with random letters, numbers, or symbols.

Safeguards

Backup Data

Backup Recovery Key

Enterprise Management

Laptops and Desktops

Full Disk Encryption

Limited Encryption

- Partition, Folder or File

Hardware Full Disk Encryption

- Automatically encrypts entire disk
- Decrypted access when an authorized user logs in
- Examples:
  - Seagate Momentus (SED)
  - Samsung SSD
  - Hitachi Self-Encrypting Drive

Operating System Encryption

Microsoft Windows

- Bitlocker
  (business versions: Vista, 7, 8, 10)
- [~~Encrypted File System (EFS)~~]
- Device Encryption
  (8.1, 10 with specific tech specs)

Apple OS X

- FileVault
- FileVault 2

Encryption Software

Full Disk & Limited

Examples:

- Check Point
- Dell Data Protection
- McAfee Endpoint
- Sophos
- Symantec (PGP and Endpoint)
- WinMagic
- ~~TrueCrypt (open source)~~

Encrypted Portable Media

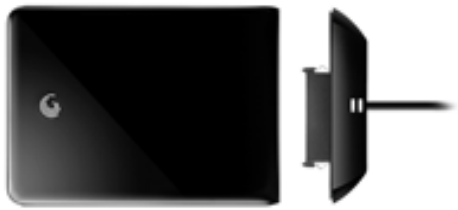
CMS Secure Vault

SanDisk

Ironkey (Imation)

Imation

Bitlocker to Go



Seagate Go-Flex

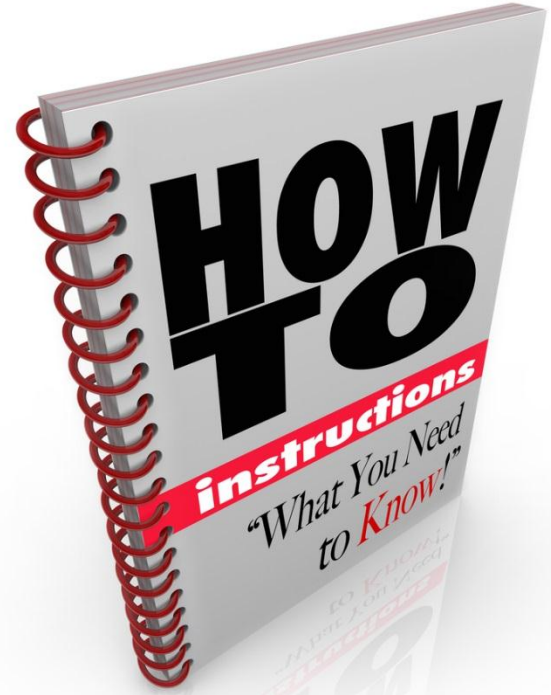
Smartphones and Tablets

iPhones and iPads

Android

BlackBerry

1. Follow manufacturer's instructions.
2. Use strong PIN or passcode.
3. Enable encryption.
4. Enable wipe after *X* failed log-on attempts.
5. Set auto timeout.



Proceed With Caution!

iTunes
For Mac + PC

Dropbox

iCloud

E-mail

SugarSync

More Secure (Examples)

boxcryptor

Dell
Data Protection
Cloud Edition

box
Business
Enterprise

SPIDEROAK

VIIVO

Sookasa

HPVoltage security

CITRIX ShareFile

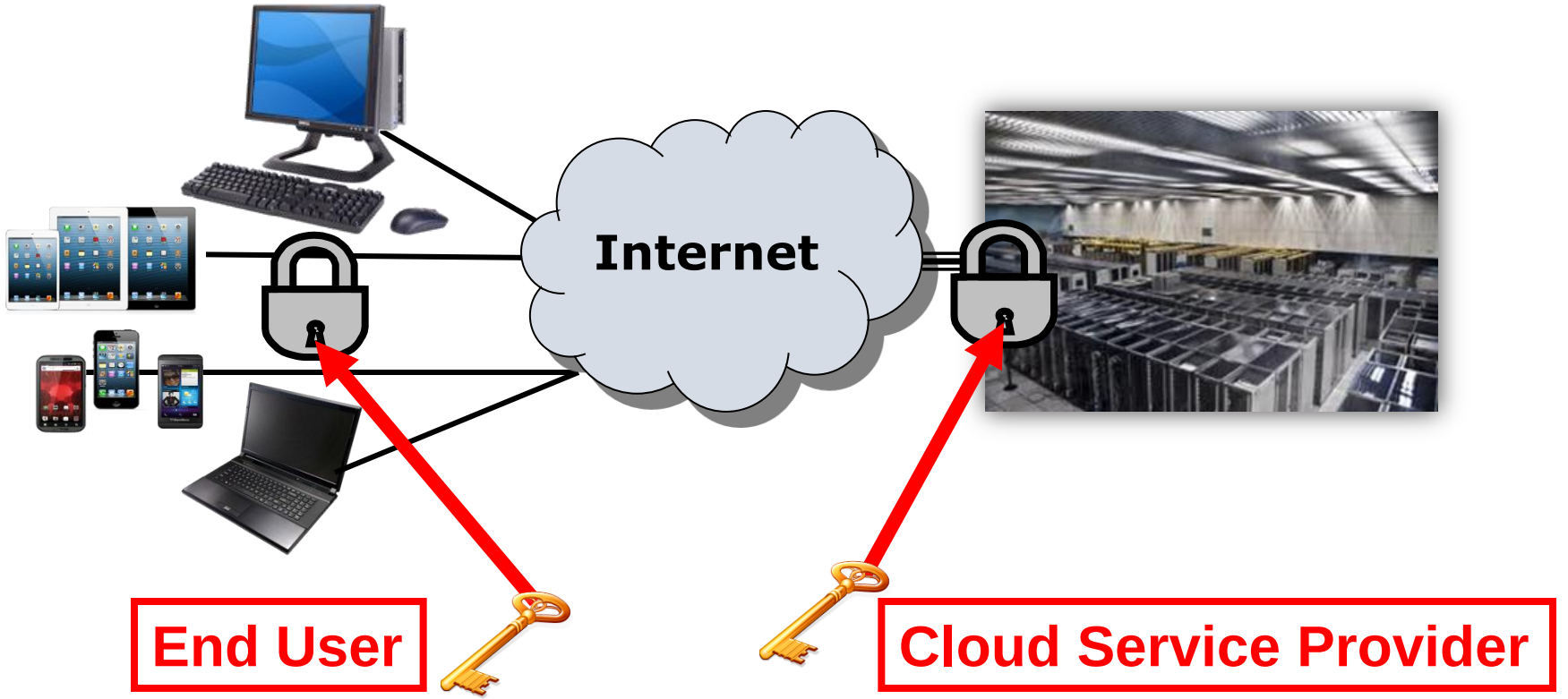
Accellion

zixcorp

BISCOM The Leader in Enterprise Document Delivery

Cloud Encryption

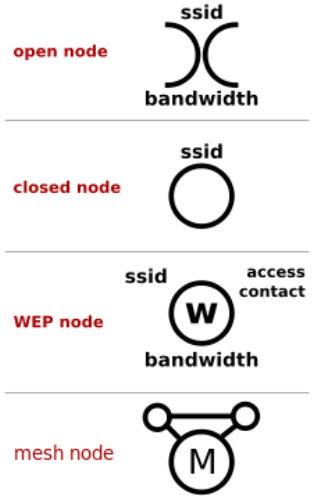
Who has the key?



Wireless Networks

- ~~[Wired Equivalent Privacy (WEP)]~~ – weak!
- ~~Wi-Fi Protected Access (WPA)~~ - cracked
- Wi-Fi Protected Access, second generation (WPA2)

- Sniffer programs
- War driving
- Pineapple
- Evil twin



Source: Wikipedia.org

Wireless Networks

“Let’s Be Careful Out There!”

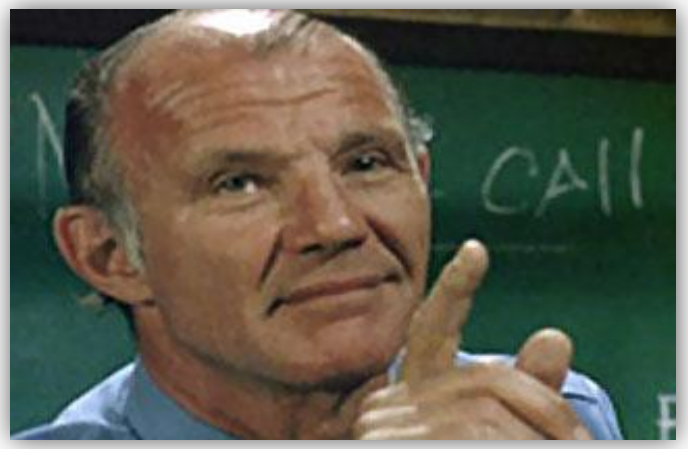
Risky if open (no need for username and password)

Be sure you have a secure connection (https: or VPN)

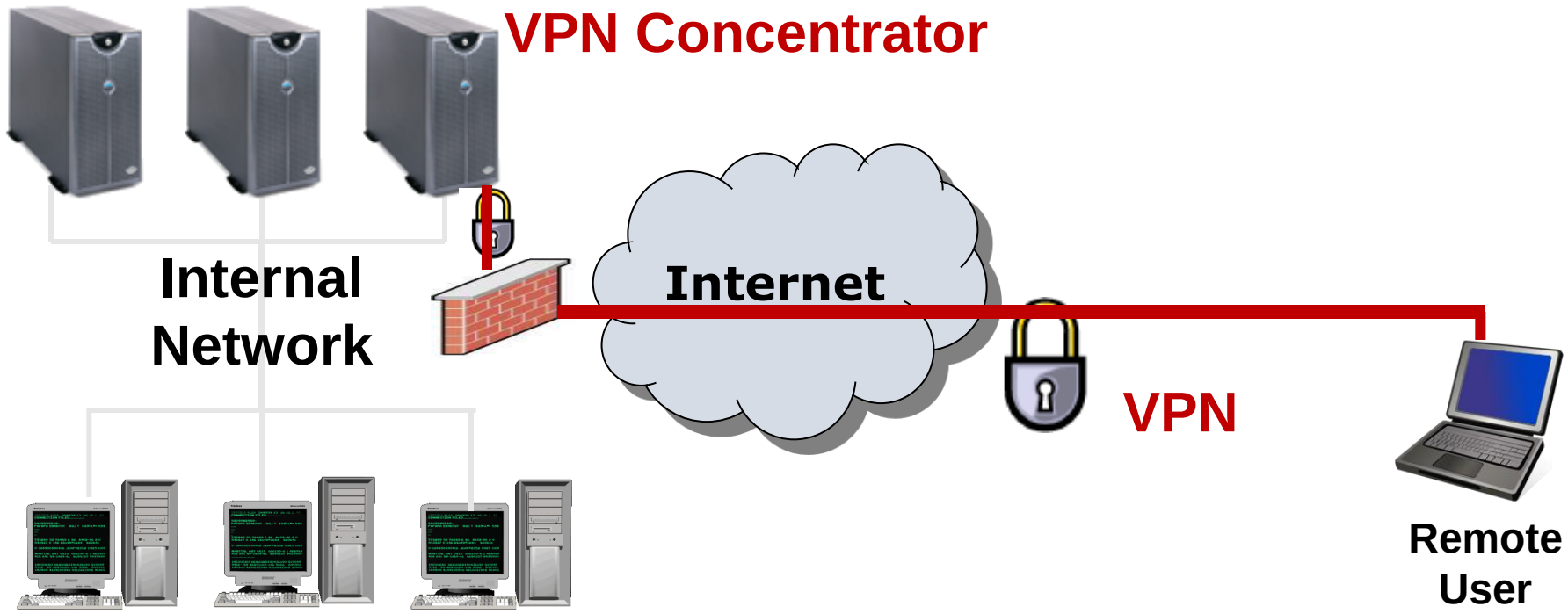
Be sure you have a properly configured firewall

Warnings from security professionals / US-CERT

Sgt. Phillip Freemason Esterhouse
Hill Street Blues



Virtual Private Network



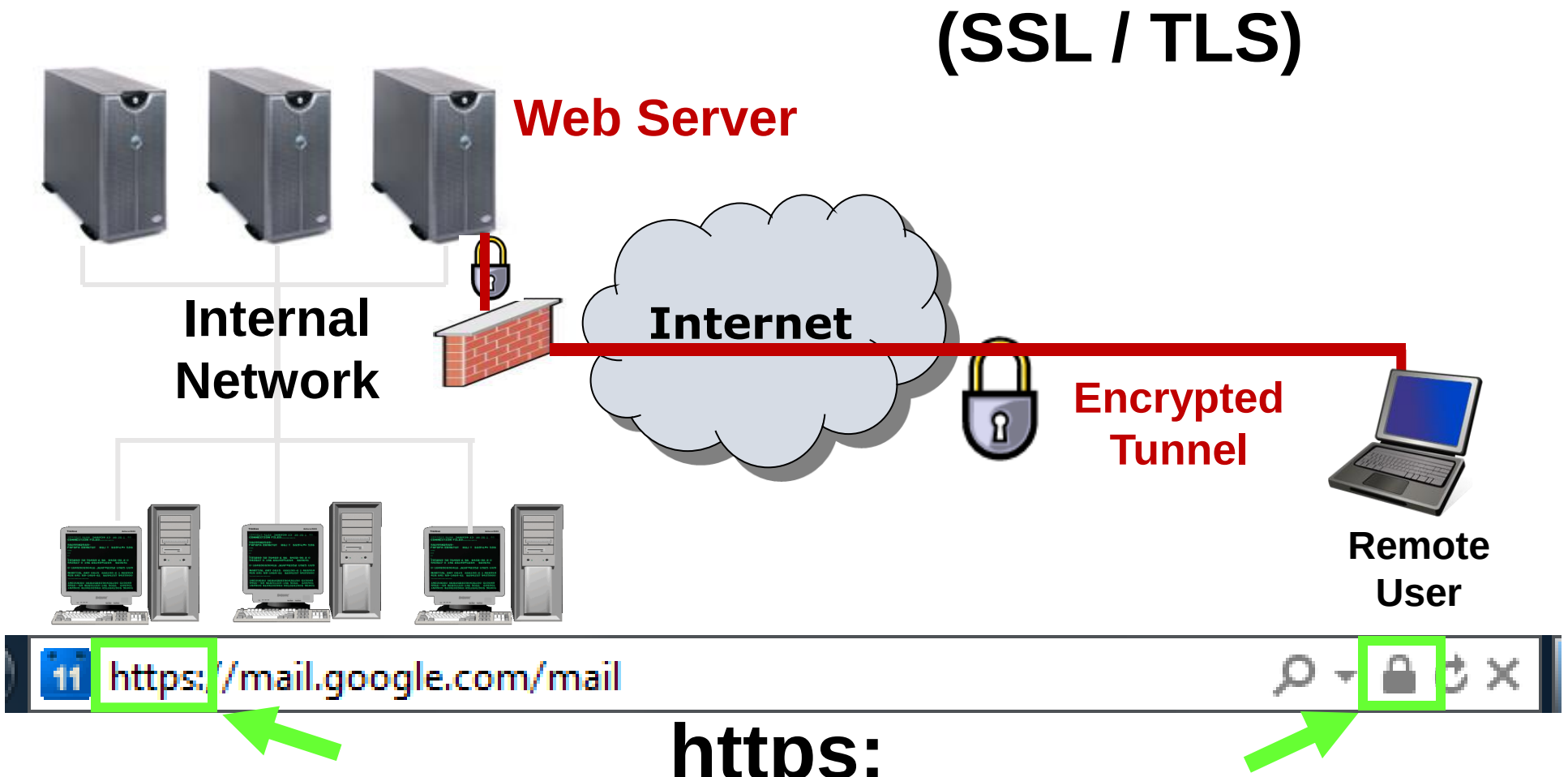
VPN Data Leaks

- IPv4 & IPv6
- IPv6 traffic leaks
- DNS hijacking
- IPv6 routing tables
- Tunnel DNS requests

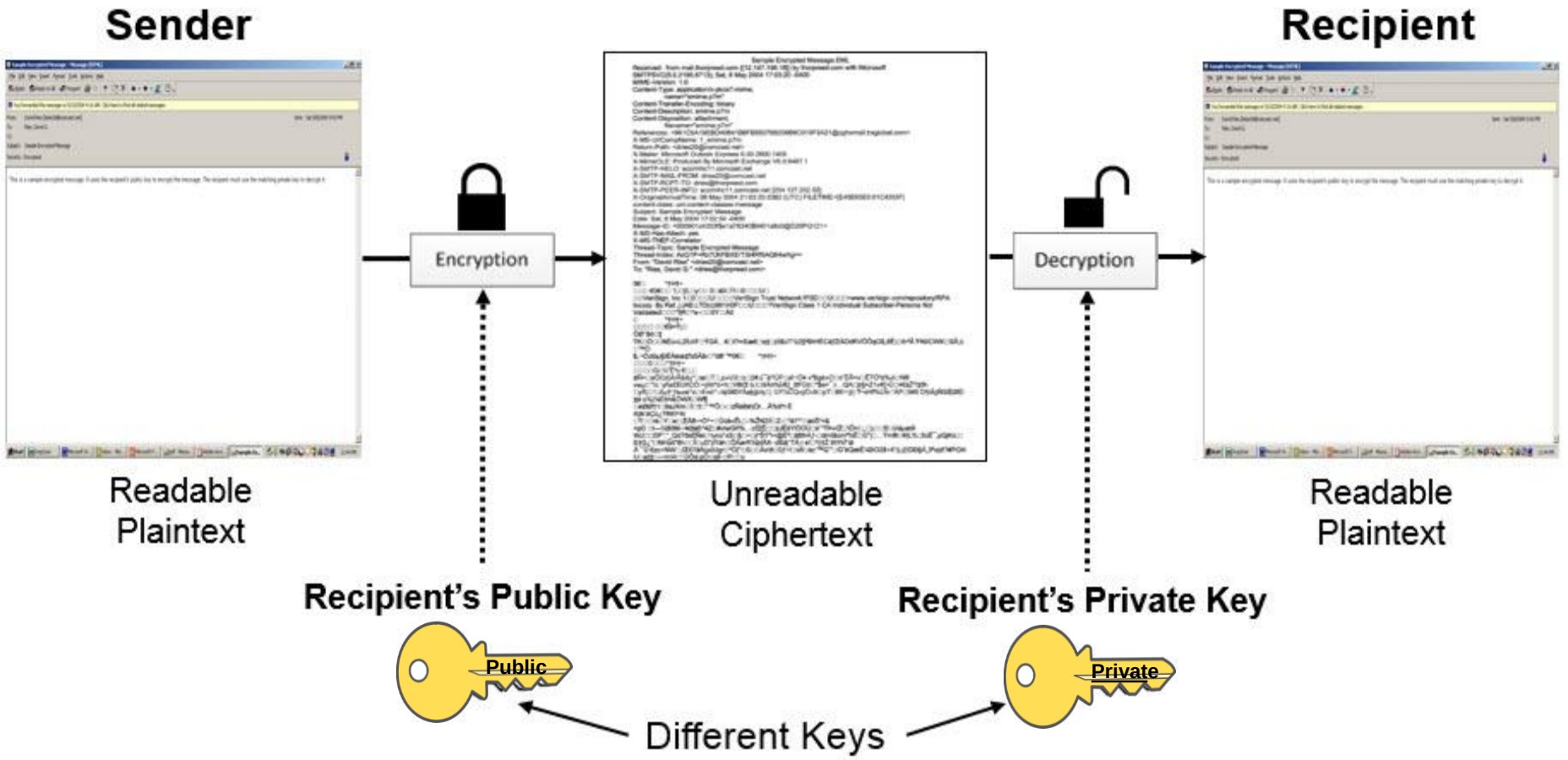
Provider	Countries	Servers	Technology	DNS	IPv6-leak	DNS hijacking
Hide My Ass	62	641	OpenVPN, PPTP	OpenDNS	Y	Y
IPVanish	51	135	OpenVPN	Private	Y	Y
Astrill	49	163	OpenVPN, L2TP, PPTP	Private	Y	N
ExpressVPN	45	71	OpenVPN, L2TP, PPTP	Google DNS, Choopa Geo DNS	Y	Y
StrongVPN	19	354	OpenVPN, PPTP	Private	Y	Y
PureVPN	18	131	OpenVPN, L2TP, PPTP	OpenDNS, Google DNS, Others	Y	Y
TorGuard	17	19	OpenVPN	Google DNS	N	Y
AirVPN	15	58	OpenVPN	Private	Y	Y
PrivateInternetAccess	10	18	OpenVPN, L2TP, PPTP	Choopa Geo DNS	N	Y
VyprVPN	8	42	OpenVPN, L2TP, PPTP	Private (VyprDNS)	N	Y
Tunnelbear	8	8	OpenVPN	Google DNS	Y	Y
proXPN	4	20	OpenVPN, PPTP	Google DNS	Y	Y
Mullvad	4	16	OpenVPN	Private	N	Y
Hotspot Shield Elite	3	10	OpenVPN	Google DNS	Y	Y

Table 1. VPN services subject of our study

Secure Connection (https:)



Email Encryption



Sample Encrypted Message.EML

Received: from mail.thorpreed.com ([12.147.198.18]) by thorpreed.com with Microsoft SMTPSVC(5.0.2195.6713); Sat, 8 May 2004 17:03:20 -0400

MIME-Version: 1.0

Content-Type: application/x-pkcs7-mime;

0€□ *†H†÷

□□□ €0€□□ 1,□}0,□y□□ 0□á0□Ì1□0□□□U□

□□VeriSign, Inc.1□0□□□U□□□□VeriSign Trust Network1F0D□□U□□□=www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)981H0F□□U□□□?VeriSign Class 1 CA Individual Subscriber-Persona Not Validated□□□"Ì|R□^s–□□ðY□:Å0

□ *†H†÷

□□□□ □□€9=Ÿ¡□

ÕØ`$è□‡

TK□Ö□□NÉú«L2ÍU/ñ'□ÝGÅ…€□t?×/£æ€□s‡□(ð$úT°ù2§²©rHÈCá¦ŒÁDdKVÔÕqG$„6Ê¡□ð•³Ã¨FN0CWK□SÃ;ù

□™Ò

$„¬ÓJiòµ§IÉÅéœ‡¾5Åã›□"ù®`™0€□ *†H†÷

□□□0□□□*†H†÷

□□□□Gí;½¨Ê³o €□,□

âÑ×□øÔEé}Å/Ã&&y"□æ□T□,p»U3□o□2#,ù¯â?ÛP□aÌ¬Ó¥·x³Bgé»O□s"ÊÃ=v□ÊTÒ³¢‰ö□N®

vwµ□"½:¨yñ±£ÊÙñCÔ:>ýW*ó+h□V®Œ·b,\□6Åh%ÎÆ[_BFÙö□*$e=¯;r…QA□þ§×Z1»K[•Ù□¤€âŽ?‡ðh

□yR¦□'□Aµ†'ƒsuœ°o□4!nó"'–ìl¢ðÌ©YÅøþjþ/q□| ¼Ÿ¼CQ«ÿÕ‹ôt□pT□8K÷'ý{-"f¬xHf%ÛÌc·"ÁP□5¥9 D†ôÎçÑSíÊØÊl

‡ä o¼}½Êôh&ÓWX□W¶

□èØØ†1□9aJXm□Í□†□*™Õ□‹□zÑáBë)Ör…Ã%šªr·Ê

A]ik'áÇü¿ÝBEFAí

□Ý□□ré□Y□e□,ËÅB~•Ò^÷□Ûúâ«ÊL□-%ŽN2íÍ□Z-□*â7^"□àôŠ¹=&

=pD □I—¾$0M-~¥žlàß^4Z□#vïwGñ%…cŒË□□ÿJÈšYlÓOÚ□é¯¹ŸÞ»Œ□\Ön□„□)¡□□6□ù\åµæ9·

WJ□□DF","_Qd7ðsÈÑè□1yno"xS□§□>□j^ŠÝ¹\+@È³□ãBÞÁƒ-□dmIãúm²¾È□Ù"|□…Ÿm®□¥}L¾:;5úÉ¯,pQjKó;□

ß†G¿"□NHûô"8h□□Î□uD¨ýŸàh□ÕÁørR½þlÅX-·dBâ|¨TÅ;(·eî□Yj†Ž 9tYhÎ"iá

Ã·¯Ù·€zc>NW□,Œ57ãÅ(µúUgr□*Ó{"□ß□□Åx\ð□0ƒ>Í□ú8□á±'™Q¨"□G¨èQæÉ¼ÐO2$+X¹ý,ý]!DÐ§Å¸3ªoÿż?#PGN

U□a{‡□‹~m¦4ì□',ÚÓd.pO□q9·□P□□y

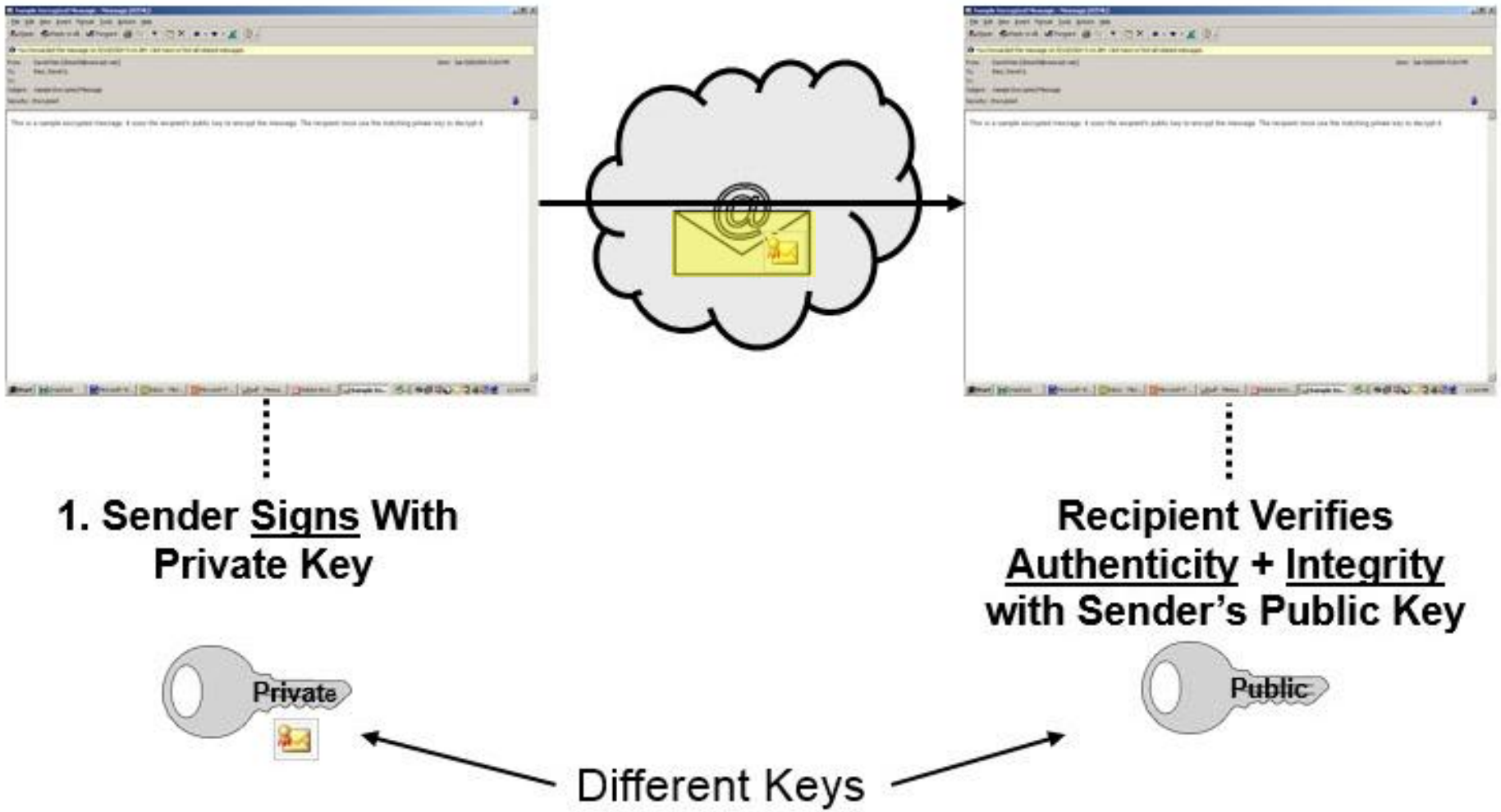
WJ□□DF","_Qd7ðsÈÑè□1yno"xS□§□>□j^ŠÝ¹\+@È³□ãBÞÁƒ-□dmIãúm²¾È□Ù"|□…Ÿm®□¥}L¾:;5úÉ¯,pQjKó;□

ß†G¿"□NHûô"8h□□Î□uD¨ýŸàh□ÕÁørR½þlÅX-·dBâ|¨TÅ;(·eî□Yj†Ž 9tYhÎ"iá

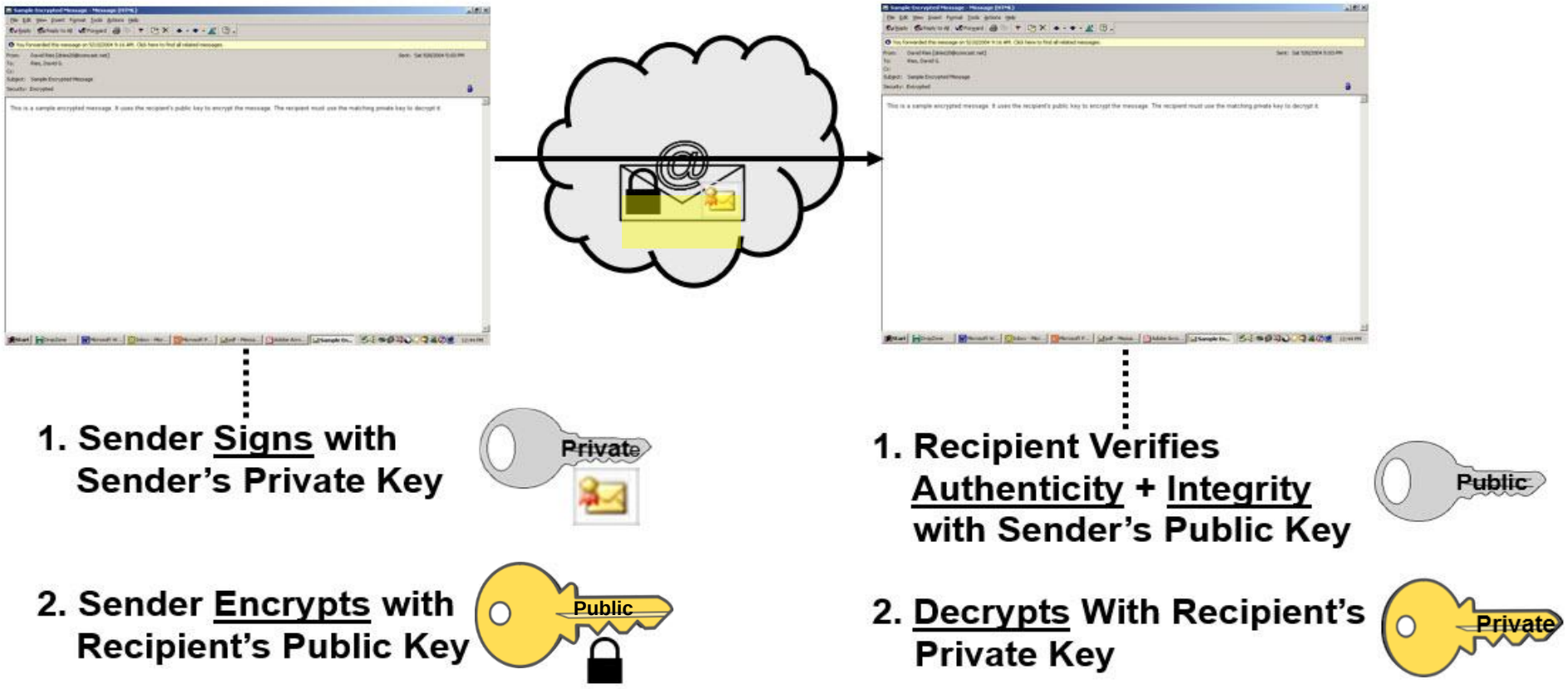
Ã·¯Ù·€zc>NW□,Œ57ãÅ(µúUgr□*Ó{"□ß□□Åx\ð□0ƒ>Í□ú8□á±'™Q¨"□G¨èQæÉ¼ÐO2$+X¹ý,ý]!DÐ§Å¸3ªoÿż?#PGN

U□a{‡□‹~m¦4ì□',ÚÓd.pO□q9·□P□□y

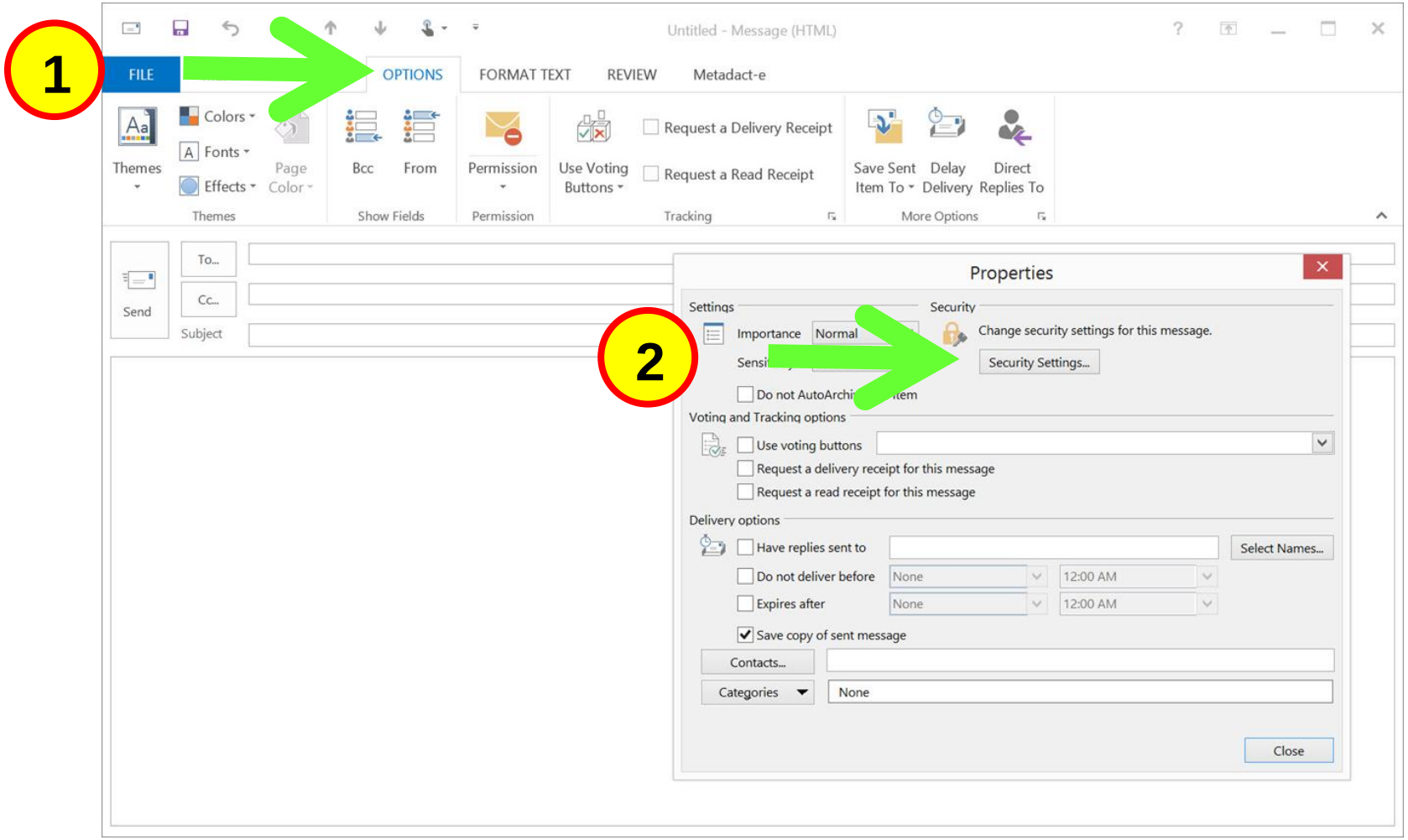
Digitally Signed Email



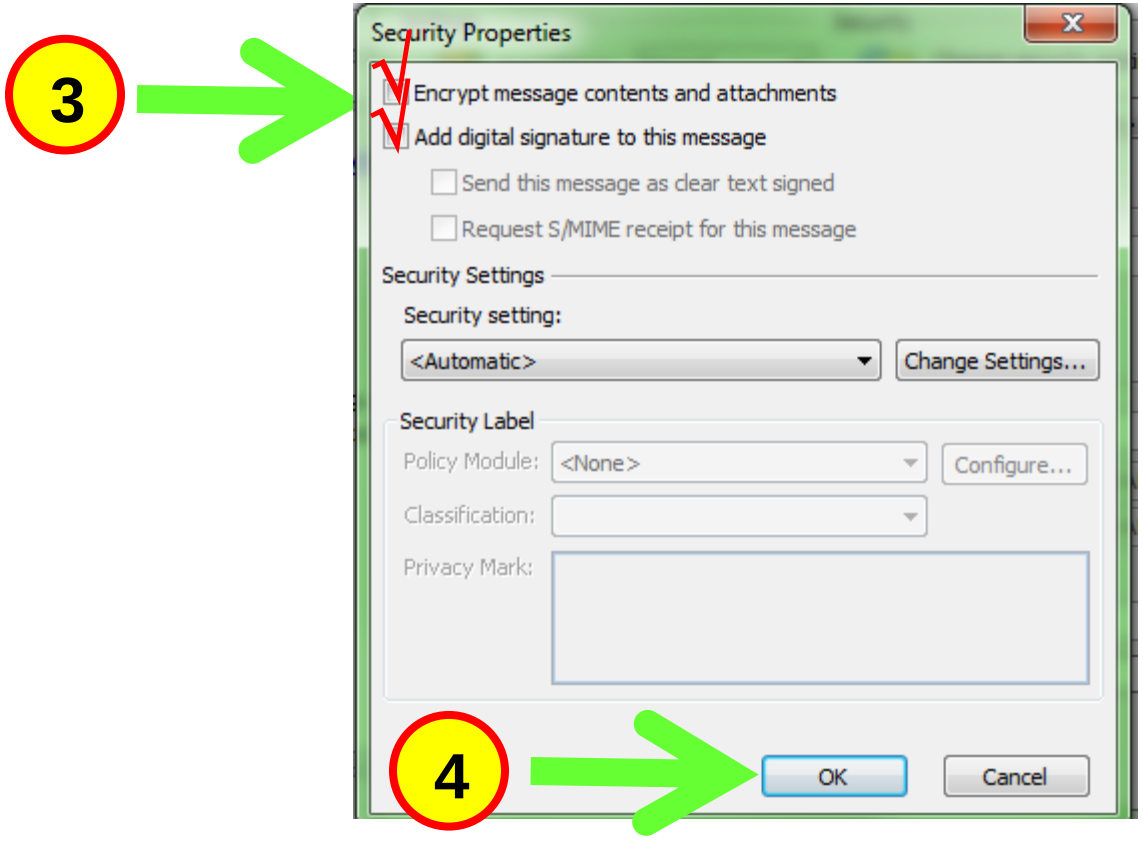
Signed and Encrypted Email



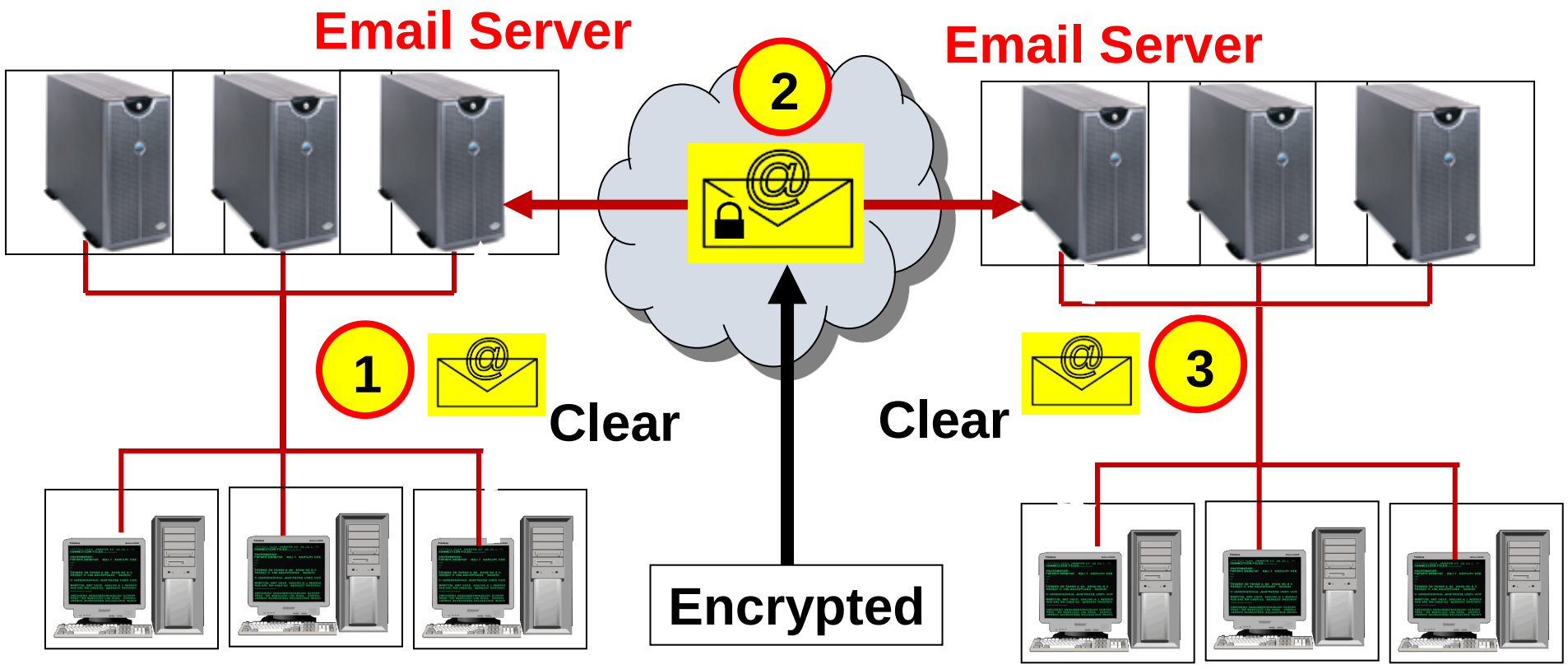
Outlook


1
Untitled - Message (HTML)
FILE
OPTIONS
FORMAT TEXT
REVIEW
Metadact-e
Themes
Colors
Fonts
Effects
Page Color
Themes
Bcc
From
Show Fields
Permission
Permission
Use Voting Buttons
Request a Delivery Receipt
Request a Read Receipt
Tracking
Save Sent Item To
Delay Delivery
Direct Replies To
More Options
Send
To...
Cc...
Subject
2
Properties
Settings
Importance
Normal
Security
Change security settings for this message.
Security Settings...
Do not AutoArchi
tem
Voting and Tracking options
Use voting buttons
Request a delivery receipt for this message
Request a read receipt for this message
Delivery options
Have replies sent to
Select Names...
Do not deliver before
None
12:00 AM
Expires after
None
12:00 AM
Save copy of sent message
Contacts...
Categories
None
Close

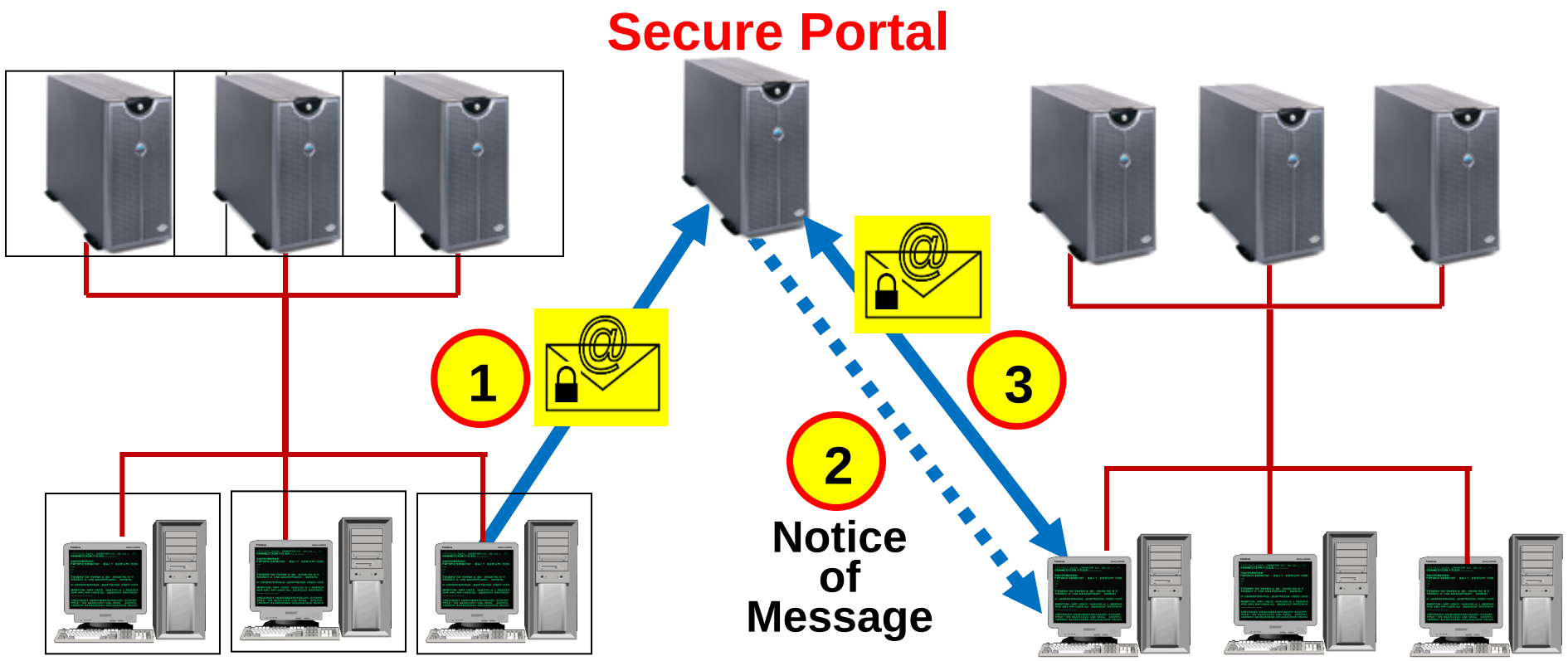
Outlook


3
Security Properties
Encrypt message contents and attachments
Add digital signature to this message
Send this message as clear text signed
Request S/MIME receipt for this message
Security Settings
Security setting:
<Automatic>
Change Settings...
Security Label
Policy Module:
<None>
Configure...
Classification:
Privacy Mark:
4
OK
Cancel

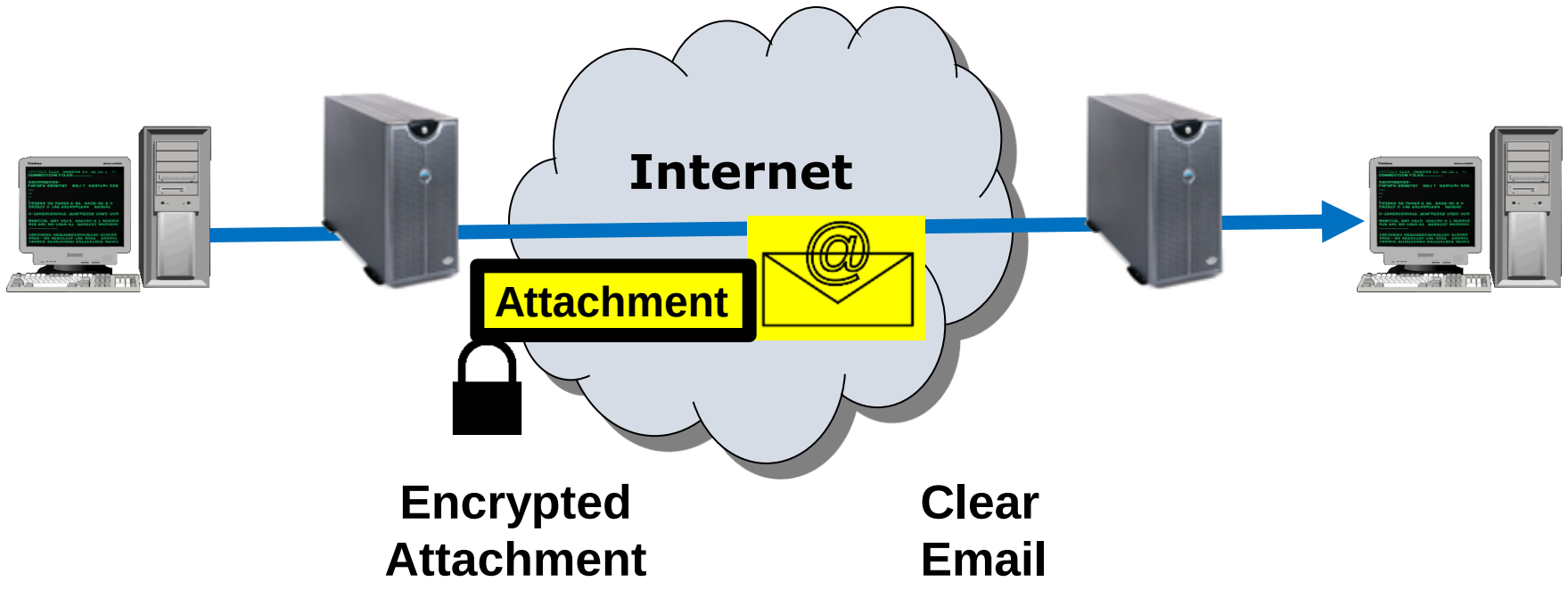
Gateway to Gateway (TLS)



Secure Portal (Pull)



Secure Attachment (Push)



Secure Email (Examples)

AppRiver

DataMotion

HP SecureMail (Voltage)

Mimecast

Office 365

Zixcorp

Encryption of Attachments

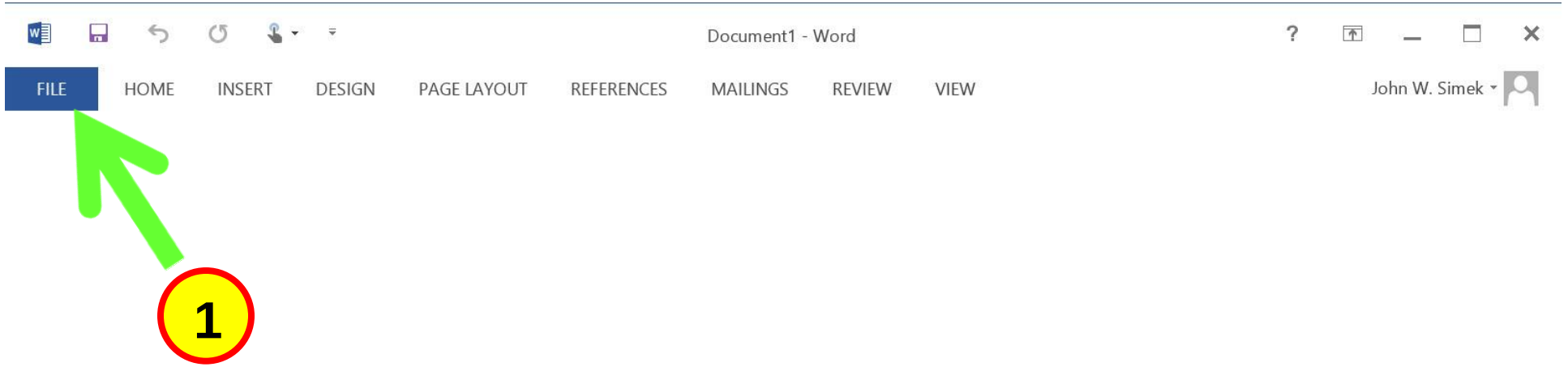
Microsoft Office

Adobe Acrobat

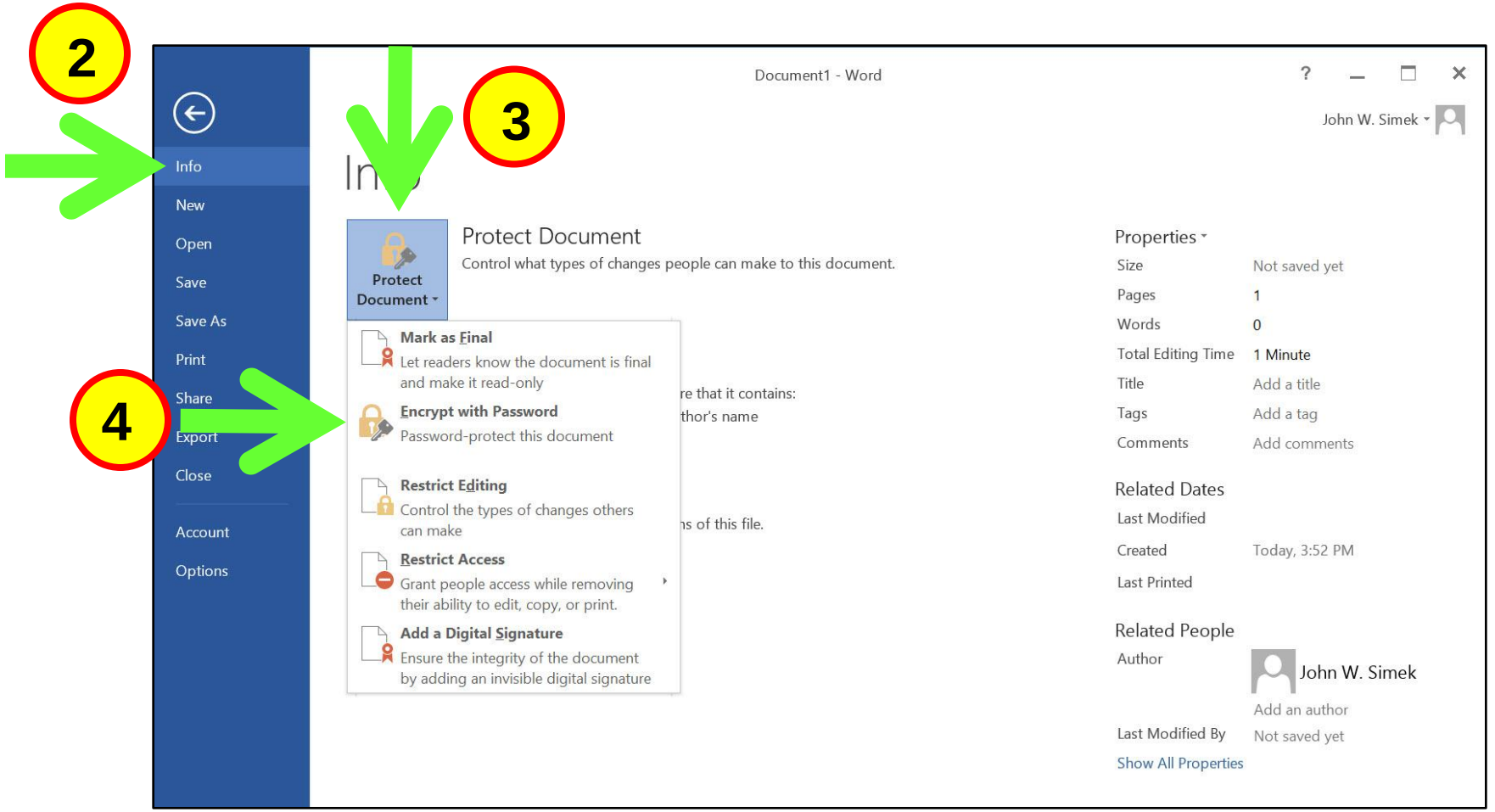
WinZip

Limited Protection!

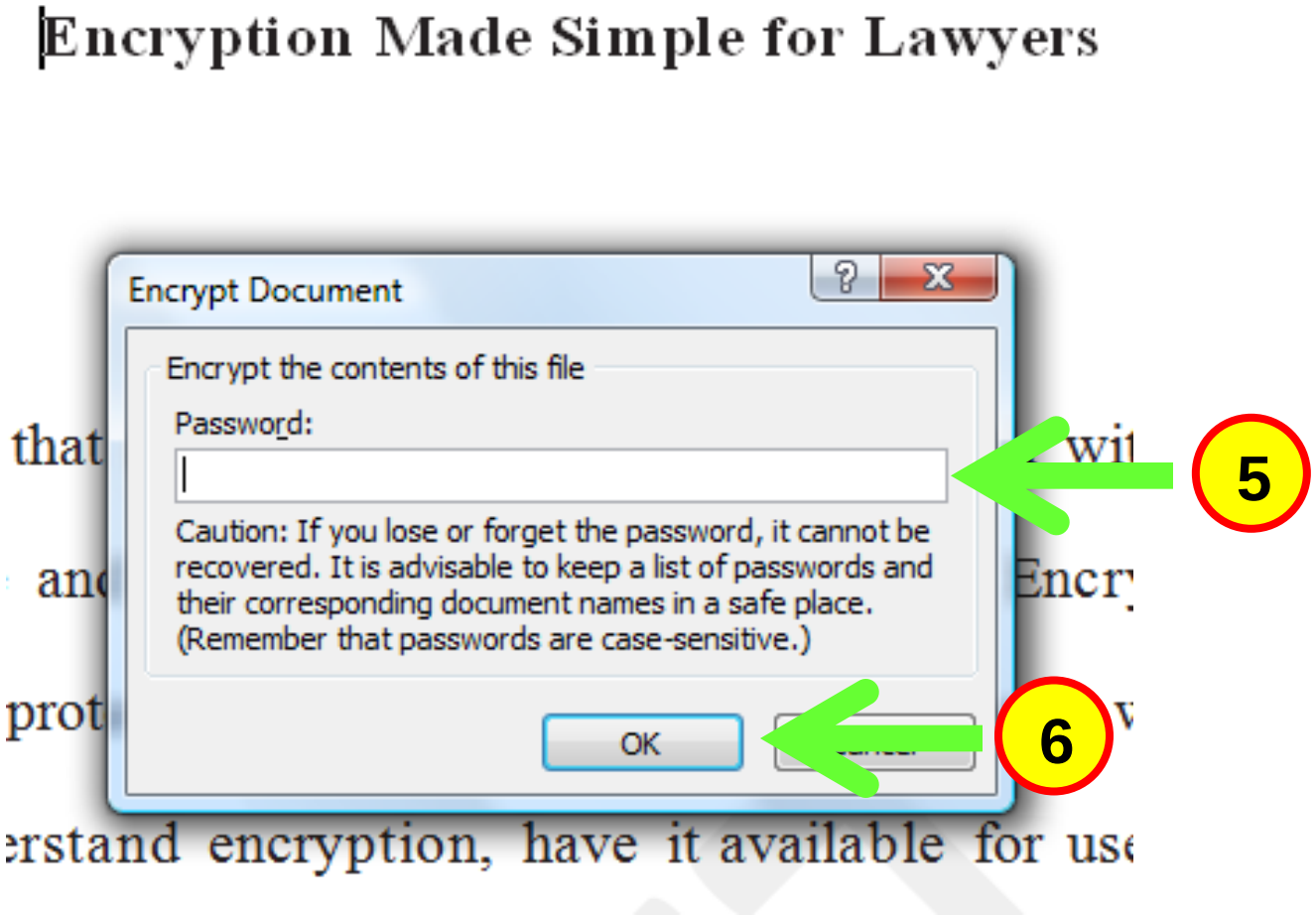
Word Menu


Document1 - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
John W. Simek
1

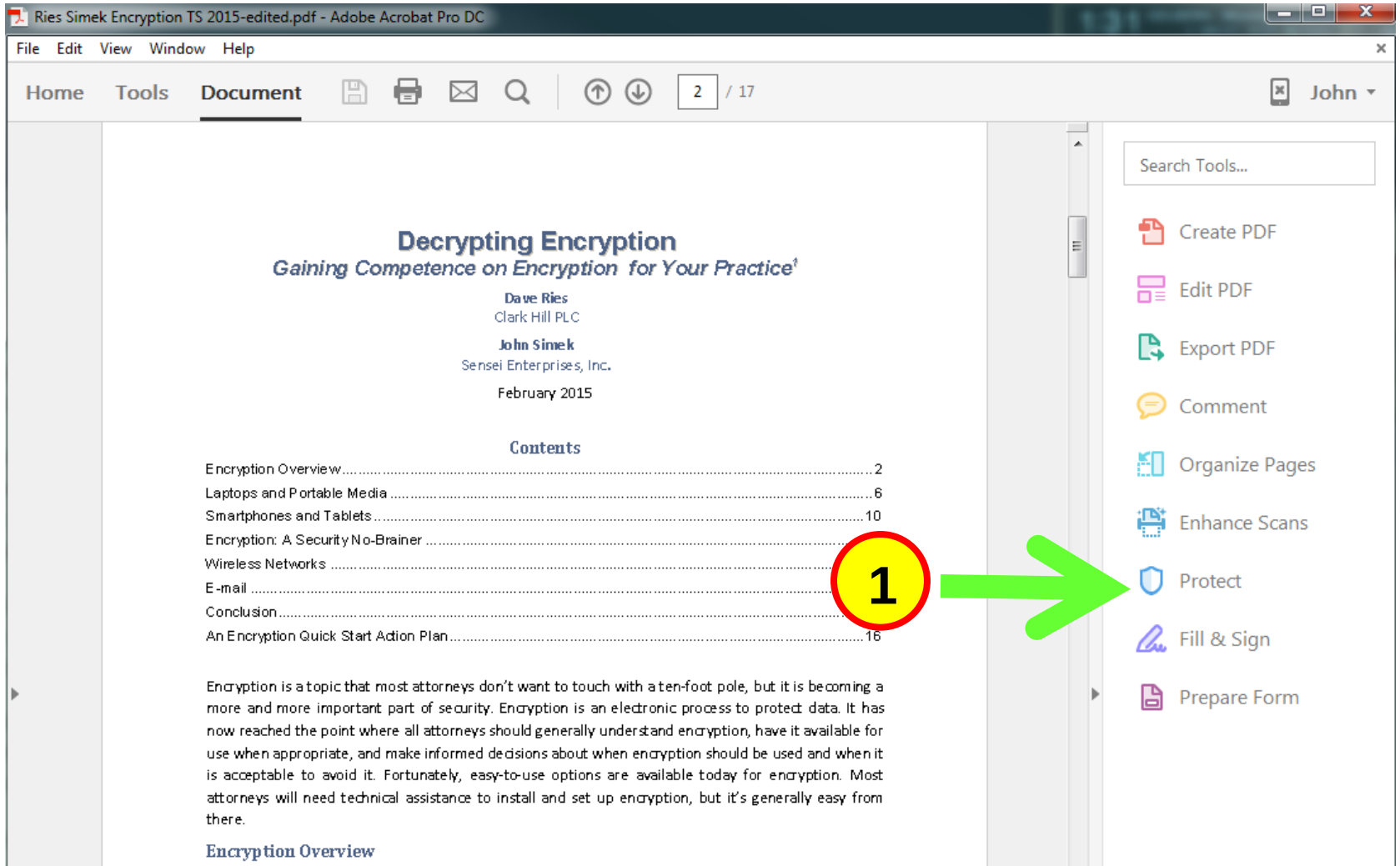
Word


2
3
4
Info
New
Open
Save
Save As
Print
Share
Export
Close
Account
Options
Document1 - Word
John W. Simek
Protect Document
Protect Document
Control what types of changes people can make to this document.
Mark as Final
Let readers know the document is final and make it read-only
Encrypt with Password
Password-protect this document
Restrict Editing
Control the types of changes others can make
Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Add a Digital Signature
Ensure the integrity of the document by adding an invisible digital signature
Properties
Size Not saved yet
Pages 1
Words 0
Total Editing Time 1 Minute
Title Add a title
Tags Add a tag
Comments Add comments
Related Dates
Last Modified
Created Today, 3:52 PM
Last Printed
Related People
Author John W. Simek
Add an author
Last Modified By Not saved yet
Show All Properties

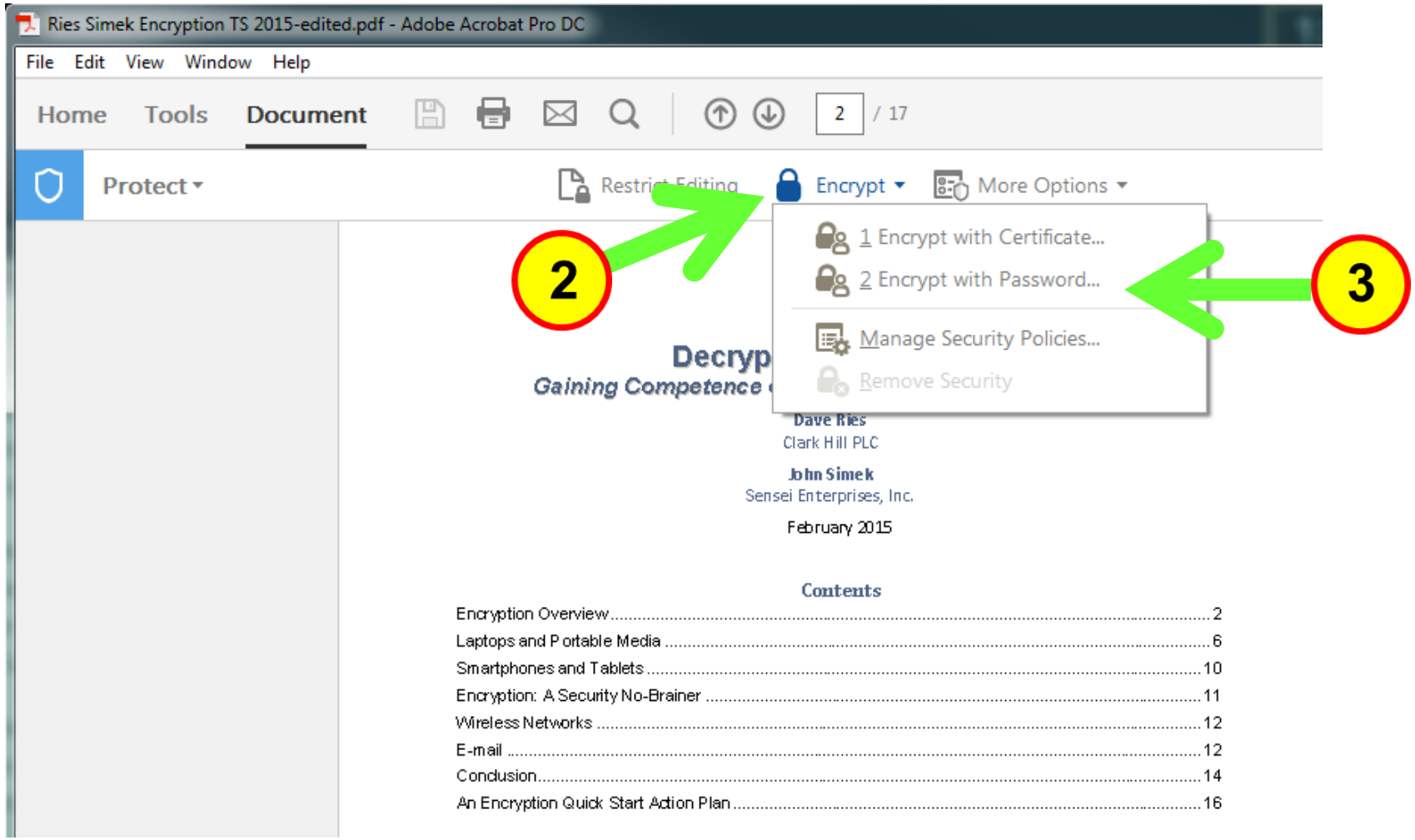
Word


Encryption Made Simple for Lawyers
Encrypt Document
Encrypt the contents of this file
Password:
Caution: If you lose or forget the password, it cannot be recovered. It is advisable to keep a list of passwords and their corresponding document names in a safe place. (Remember that passwords are case-sensitive.)
OK
5
6
that
wit
and
Encry
prot
erstand encryption, have it available for use

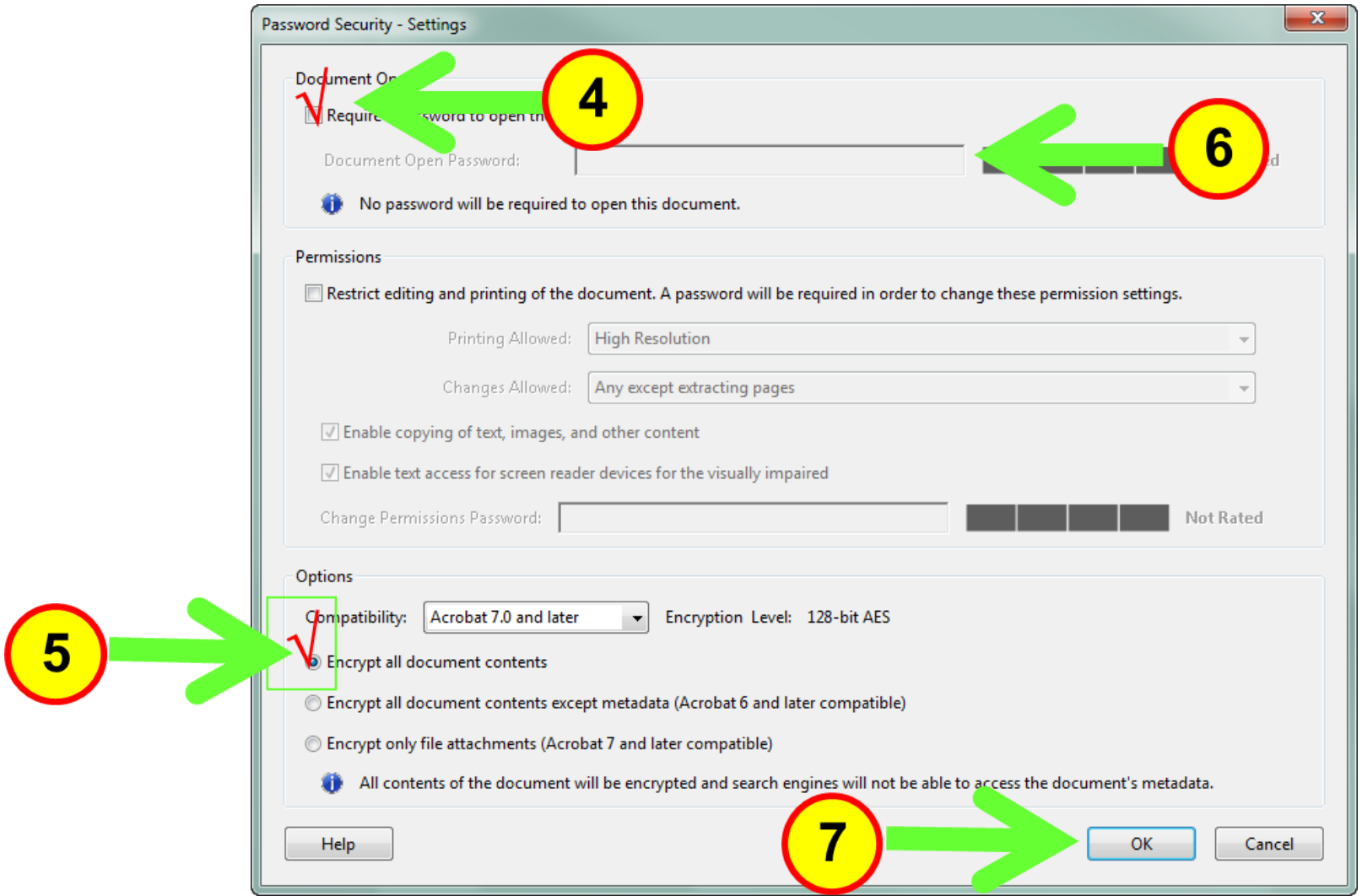
Adobe Acrobat



Adobe Acrobat

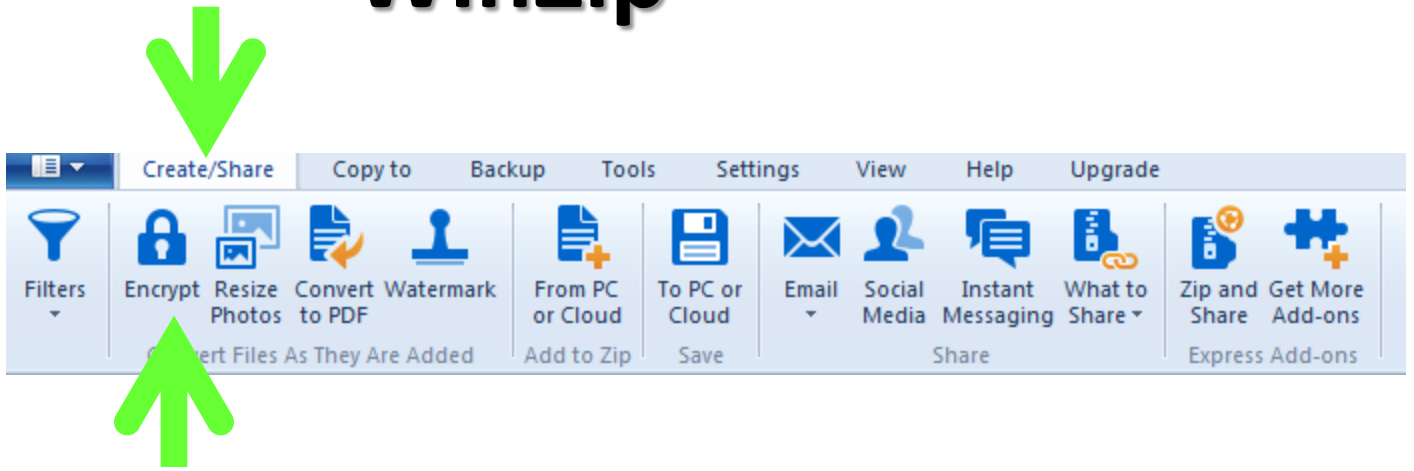


Adobe Acrobat

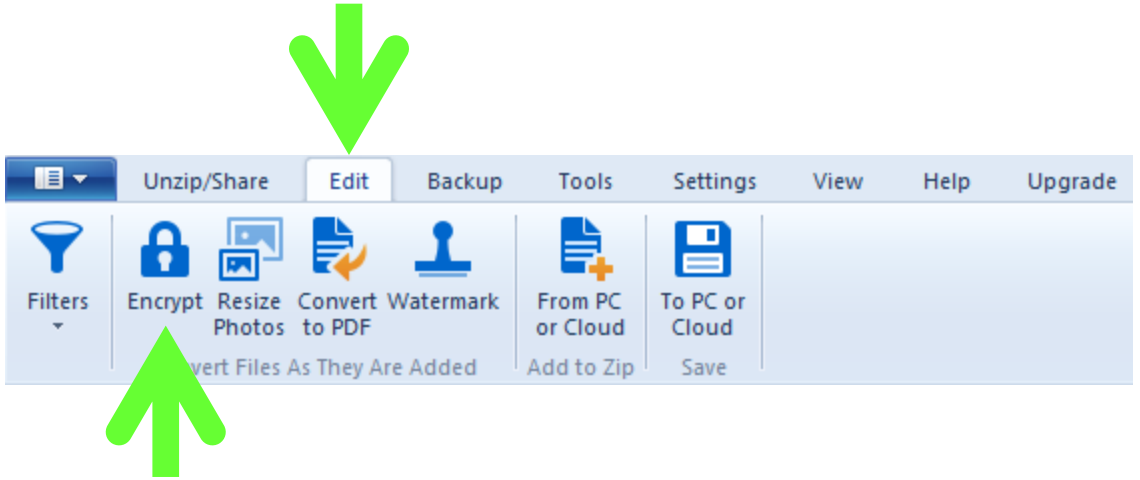


WinZip

New File



Existing File



When Encryption is Bad

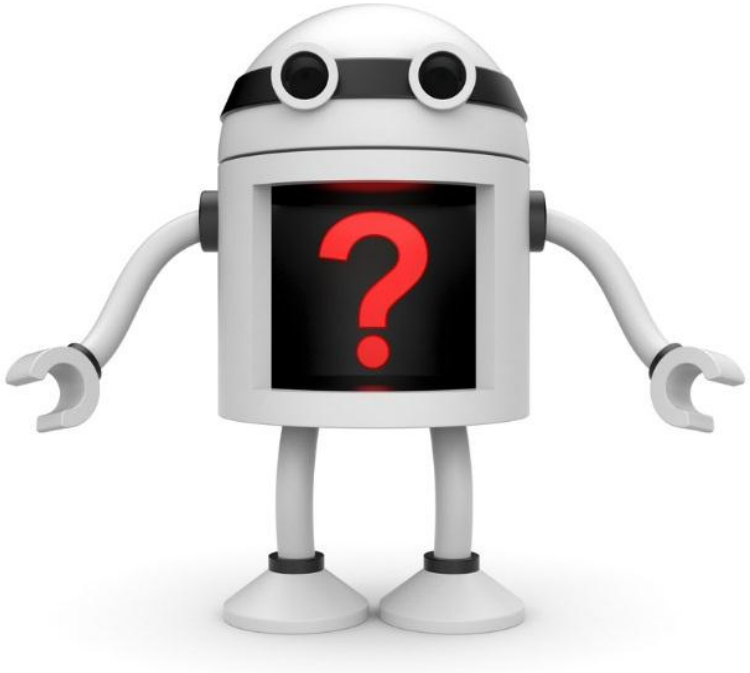
- SSL/TLS – network attacks
- Cyber criminals
- Encrypted C&C communications
- IDS/IPS “blind”

Encryption is part of the solution.

Use with other comprehensive security measures.

BACKUP!

Key recovery

Enterprise management

Questions