

# DATA ENCRYPTION

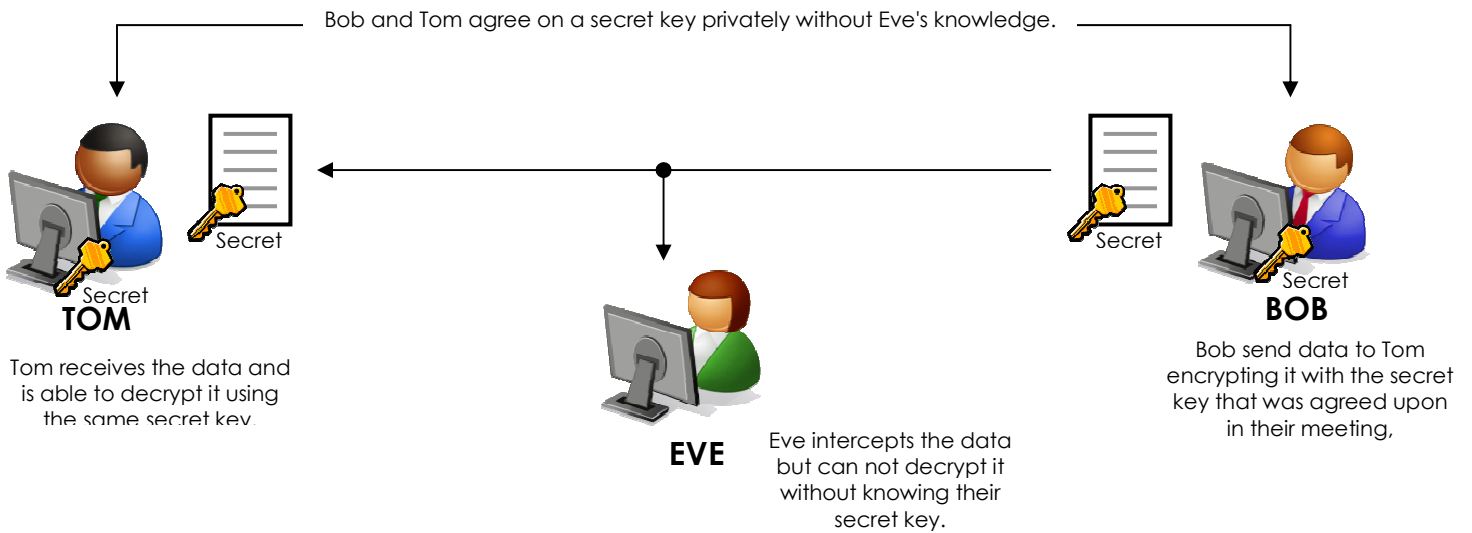
## What is Data Encryption?

Data encryption is a secure process for keeping sensitive and confidential information private. Using Data Encryption makes the file unreadable unless it is decrypted, usually using a pass-phrase (key).

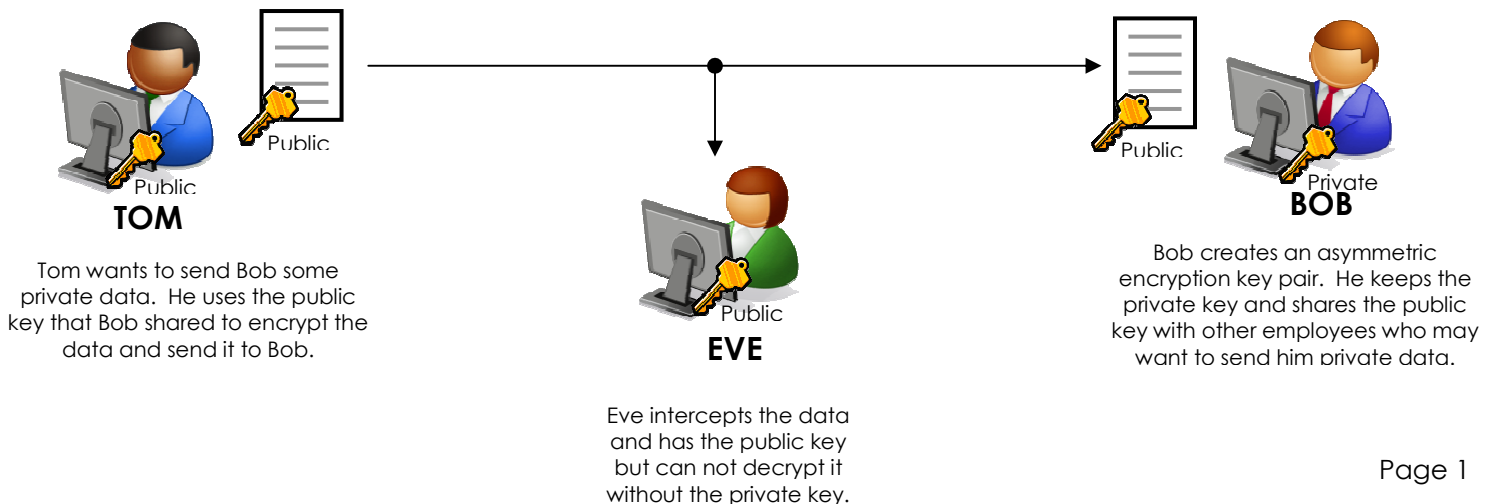
## Main Types of Data Encryption

Symmetric encryption is the oldest and best-known data encryption method. A secret key (word, number, or random string of characters) is applied to data to change the context and make it cryptic without the key. The sender and receiver of symmetric encryption must have the same key in order to encrypt and decrypt the data. The issue with this type of encryption is sharing these keys over the internet or a large network without them being discovered by the wrong individuals. *Note: All the applications to follow will use this type of encryption.*

Best practice in this scenario is to agree on the secret key before hand, next would be to call that individual over the phone and give them the secret key directly. Never under any circumstances email a secret key. If an attacker, such as Eve, can intercept your email message then they can intercept a secret key. This type of intrusion is called a "Man-in-the-Middle" attack.



Asymmetric encryption is one answer to this problem; it creates a key pair, one private and one public. The private key is kept secret and only the originator should know it. The public key, however, can be shared with anyone who wishes to send the originator of the key encrypted data. Asymmetric encryption's "one-way" path allows it to be more secure, because only the individual holding the private key can decrypt the data and doesn't have to share a "secret" password with anyone else. A reverse version of this cryptography is used in Digital Signatures.



### Some Basic Encryption Issues to Remember:

1. **THERE IS NO WAY TO BE 100% PROTECTED.** There are numerous tools, utilities, and instructions describing how to decrypt data. The goal of encryption is to make things harder to access so that individuals will leave the data alone. In a school setting the methods discussed below should work fine to protect your data and deter individuals from accessing confidential information.
2. **RULES FOR SECRET KEYS.** A general rule for creating a secret key is to make them 6-8 characters in length and have them contain numbers, letters, and symbols. (Some applications don't allow a user to use symbols and restrict the length, apply as much of the above rule as possible). Avoid using secret keys such as birth date, address, phone number, family names, pet names, etc; these are common and attackers will try these first. Finally you should never write down your passphrase; it is the easiest way for an attacker to steal confidential information.
3. **KEEP AN UNENCRYPTED BACKUP.** It is best practice to keep an unencrypted backup of your data in a secure location off-site in case it is deleted or the password is forgotten. While there are third-party software options that protect against file deletion, most standard options do not.

## **ENCRYPTING DATA OVER EMAIL \ NETWORK**

As a Network Technology Consultant and Data Manager I understand how important it is to secure sensitive data. I have worked with the school-system for several years now creating, managing, and networking database software and the one issue that always arises is, will my data be secure? This especially holds true for the Exceptional Children's Department where unsecured data can become a lawsuit against the teacher and the school-system because the files and information handled is strictly confidential to the individual child. According to IDEA Sec. 300.610 - Confidentiality, which reads, "...to ensure the protection of the confidentiality of any personally identifiable data, information, and records collected or maintained...by LEAs"<sup>1</sup> we have a responsibility to maintain that child's privacy and are bound by state mandate to do so.

Due to these regulations I have found the following freeware software extremely useful to help me stay compliant when transferring sensitive and confidential documents electronically.



**IZARC** (<http://www.izarc.org>) is a Windows compatible archive utility that will compress and secure your data with a strong 256-bit AES standard encryption. The software can be used freely for both personal and commercial use. I have also found it helpful when sending data to out-side agencies that are using WinZip, a commercial compression utility, by using IZARC's PK ZIP v2.0 encryption type I can create a compatible file. IZARC has many features to offer and has been rated Excellent in Editor's Review at Softpedia. The following site contains step-by-step instructions on how to use the IZArc Archiver, <http://www.izarc.org/tutorials.html>.

Once I have compressed (made the file smaller, more suitable for email) and encrypted (password-protected) the data I attach it to my email and send it. If I have not made arrangements with the individual prior to sending the data, I state somewhere in the email for them to call me for the password. I include my office phone and I also reference the attachment in the body of the email, example:

Mr. Smith -

I have attached the data you requested...please call me at my office between the hours of 7am and 3pm for the password. My office number is ###-#### x ####.

Attachments:

compressed\_data.zip

Thanks

*My contact information - email signature*

---

<sup>1</sup> See Building the Legacy: IDEA 2004, especially Sec. 300.610 - 300.627, which deal with Confidentiality (<http://idea.ed.gov/explore/view/p/%2Croot%2Cregs%2C300%2CF%2C>).

# ENCRYPTING A MICROSOFT OFFICE DOCUMENT - Word, Excel, PowerPoint

Inside an open Microsoft Office Document password and encryption options are accessible in the Security tab;

Step 1: From the Menu Bar select Tools → Options (Figure 1.1)

Step 2: From the Options Window select the Security Tab (Figure 1.2)

Type a desired password in the "Password to Open"

Click the "Advanced..." button

Step 3: Select the Encryption Type and Key Length desired. (Figure 1.3)

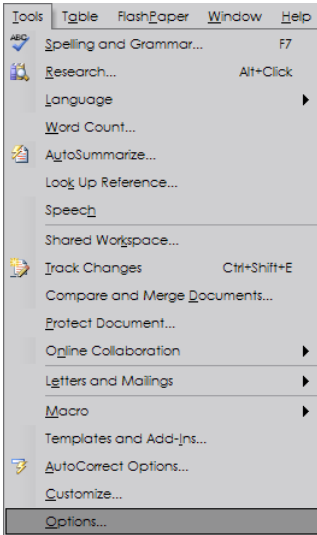


Figure 1.1

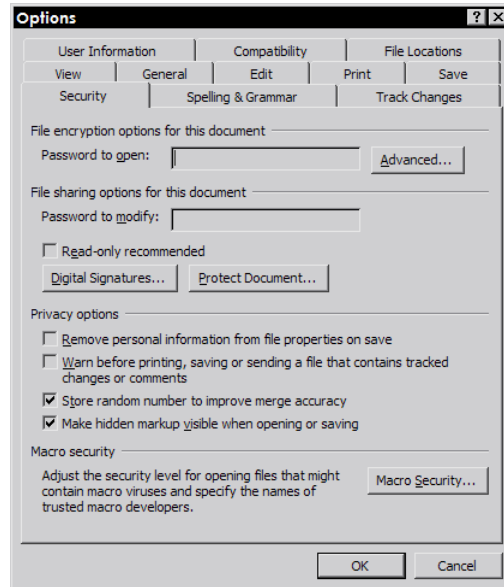


Figure 1.2

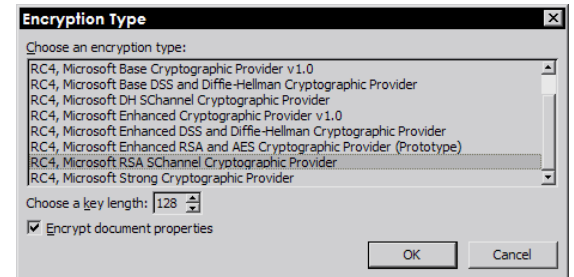


Figure 1.3

**Note** the further down the list you go on Encryption Type the high number the Key Length the stronger the encryption. A 128-bit Encryption Key is the highest you can have for this application.

An alternative to this method can be accessed through the Save As... command

Step 1: From the Menu Bar select File → Save As (Figure 2.1)

Step 2: From the Save As... Window select Tools → Security Options [General Options in Excel] - (Figure 2.2)

Step 3: Type a desired password in the "Password to Open" (Figure 2.3)

Click the "Advanced..." button

Step 4: Select the Encryption Type and Key Length desired. (see Figure 1.3 above)

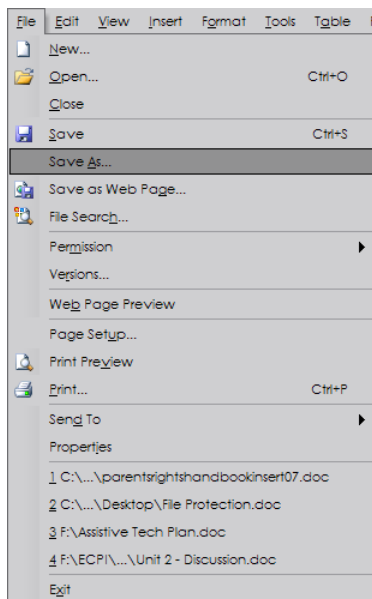


Figure 2.1

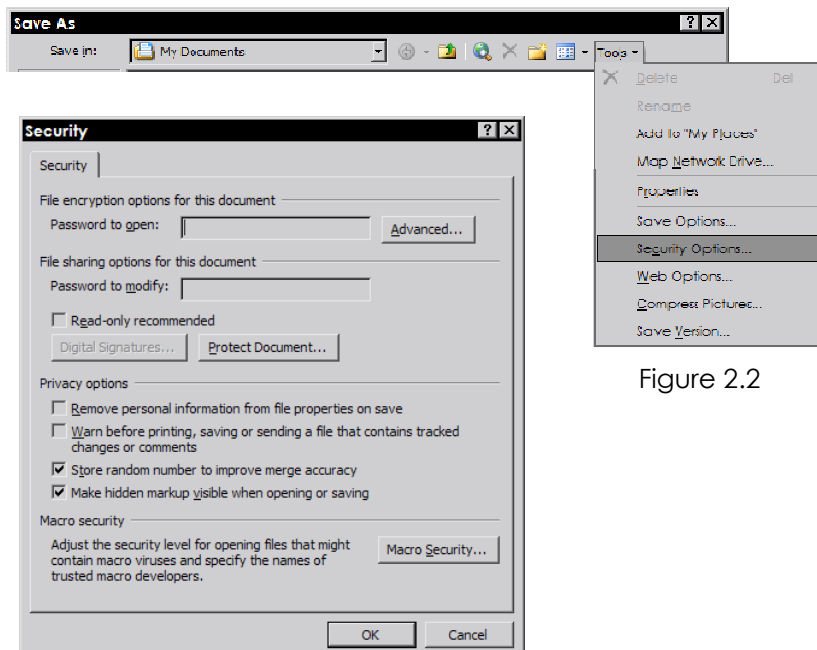


Figure 2.2

## SETTING THE DEFAULT ENCRYPTION TYPE VIA WINDOW'S REGISTRY FOR MICROSOFT OFFICE

Figure 2.3

Be advised changing registry keys can cause applications to stop working if not done correctly. Only do this if you feel comfortable with modifying the Windows Registry.

You can set a default encryption type for all Office applications that use encryption methods by adding a registry value to the Windows Registry. The default encryption algorithm for a standard installation is not the strongest possible and if you constantly encrypt your Office documents, it is advisable to set a higher level of encryption to default, then manually setting it each time.

To set the default encryption type, open the Registry editor

Step 1: Click START → RUN... (Figure 3.1)

Type "regedit" at the prompt

Step 2: Navigate to HKEY\_CURRENT\_USER\Software\Microsoft\Office\11.0\Common (Figure 3.2)

Step 3: Inside the Common Folder create a new Key called Security (Figure 3.3 - Figure 3.4)

Step 4: Inside the Security Folder create a new Multi-String value called "DefaultEncryption" (Figure 3.5)

Step 5: Set the value to: (Figure 3.6)

Encryption Provider = Microsoft RSA SChannel Cryptographic Provider

Encryption Type = RC4

Key Size = 128

These values can be obtained from the Advanced menu in the Security tab. Values should resemble Figure 3.4

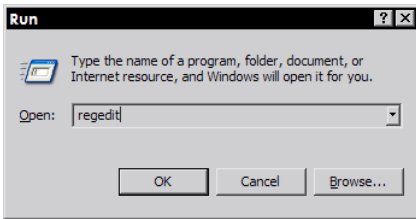


Figure 3.1

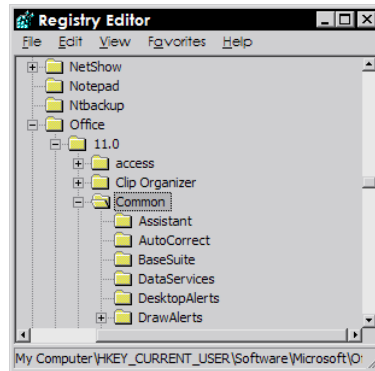


Figure 3.2

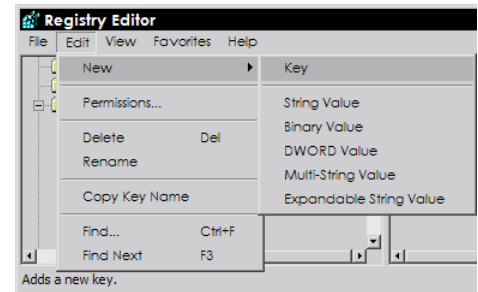


Figure 3.3

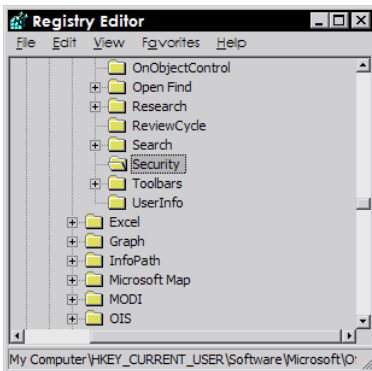


Figure 3.4

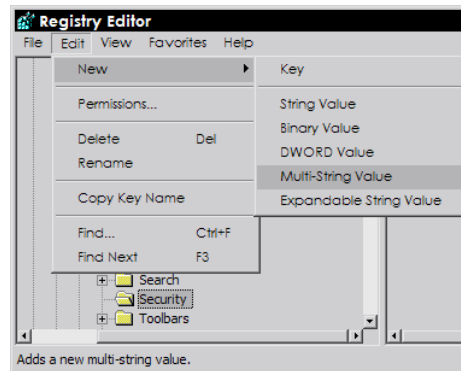


Figure 3.5

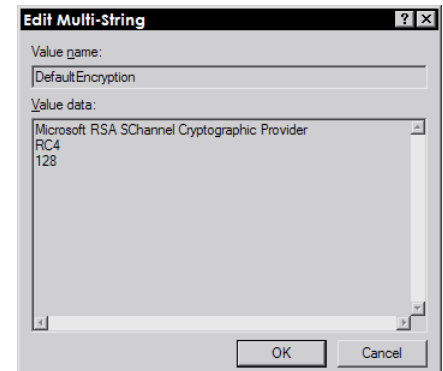


Figure 3.6

# ENCRYPTING AN ADOBE ACROBAT PDF DOCUMENT

-- You must be running Adobe Acrobat Standard or Professional not Reader --

These instructions are based off of Adobe Acrobat 8 Professional:

Step 1: From the Menu Bar select Advanced → Security → 2 Password Encrypt... (Figure 4.1)

Step 2: A message will appear asking "Are you sure you want to change the security on this document?"  
Click Yes (Figure 4.2)

Step 3: Inside the Password Security - Settings Window you can do several things: (Figure 4.3)

- Select the Compatibility: this means which versions of Adobe Acrobat do you want this document to be able to be opened. (Recommended Adobe Acrobat 5.0 and later, this sets the encryption to 128-bit RC4).
- Check "Require a password to open the document" → Type a password in the Document Open Password field.
- Click OK

Step 4: Adobe Acrobat will prompt you to confirm the password by typing it again → Click OK (Figure 4.4)

Step 5: You will be prompted "Security settings will not be applied to the document until you save...", so save the document now, from the Menu Bar select File → Save As... (Figure 4.5)

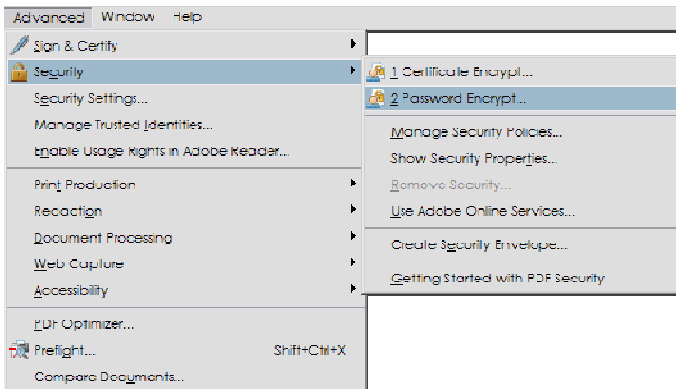


Figure 4.1

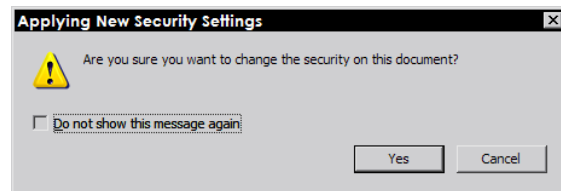


Figure 4.2

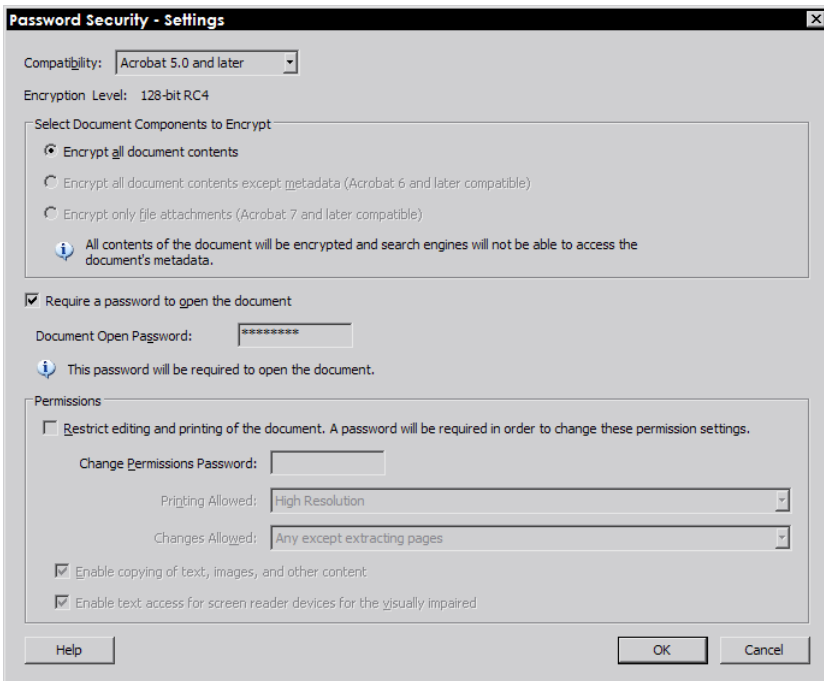


Figure 4.3

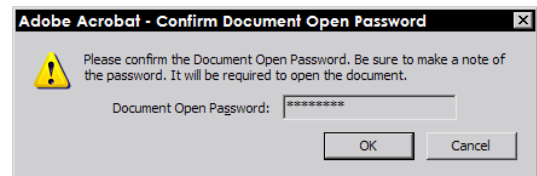


Figure 4.4

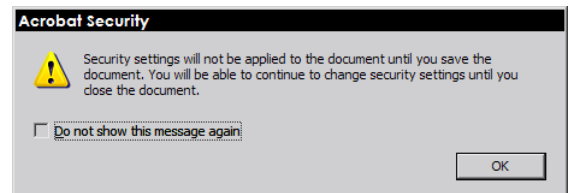


Figure 4.5