

# *Safe and Secure Online Transactions*

**Gavin Bartholomew**  
**Senior Systems Engineer**

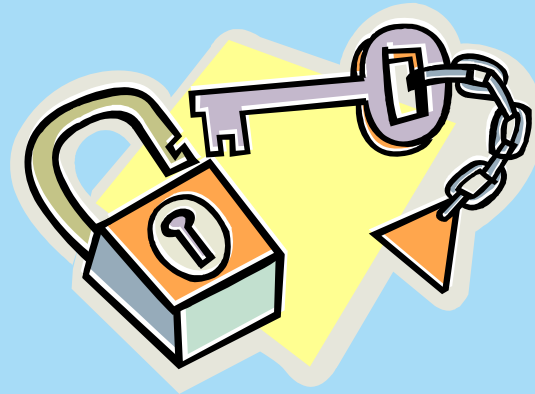


# Encryption

- To put into code or cipher.
- *Computer Science* To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties
- i.e. – password protected
- Symmetric vs. Asymmetric

# Symmetric Encryption

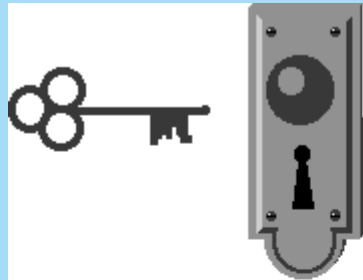
- One key to “lock” and “unlock” the file
- Both the sender and receiver need to possess the same key



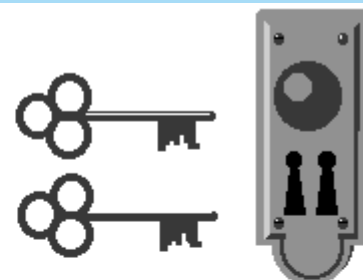
# Asymmetric Encryption

- Uses 2 keys (passwords)
- Public / Private Key Pair
- Encrypt with one, decrypt with the other





**Symmetric  
(Conventional)  
One Key  
Used for both  
Encryption  
and  
Decryption**



**Asymmetric  
(Public Key)  
Two Keys  
One Key Used  
for Encryption  
and  
One Key Used  
for Decryption**

# Public Private Key Example

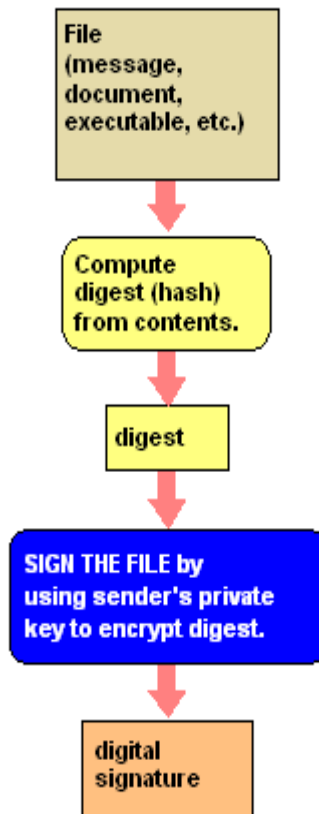


# Non- repudiation

- The message originated from A (the only person who could have encrypted the digest correctly) - *origin*
- The message has not been altered in transit. - *delivery*

# Digital Signatures

From Computer Desktop Encyclopedia  
© 2005 The Computer Language Co. Inc.



The digital signature is an encrypted digest of the file (message, document, driver, program) being signed. The digest is computed from the contents of the file by a one-way hash function such as MD5 or SHA-1 (see [MD5](#) and [SHA-1](#)) and then encrypted with the private part of a public/private key pair (see [RSA](#)). To prove that the file was not tampered with, the recipient uses the public key to decrypt the signature back into the original digest, re-computes a new digest from the transmitted file and compares the two to see if they match. If they do, the file has not been altered in transit by an attacker.

# Certificate Authorities

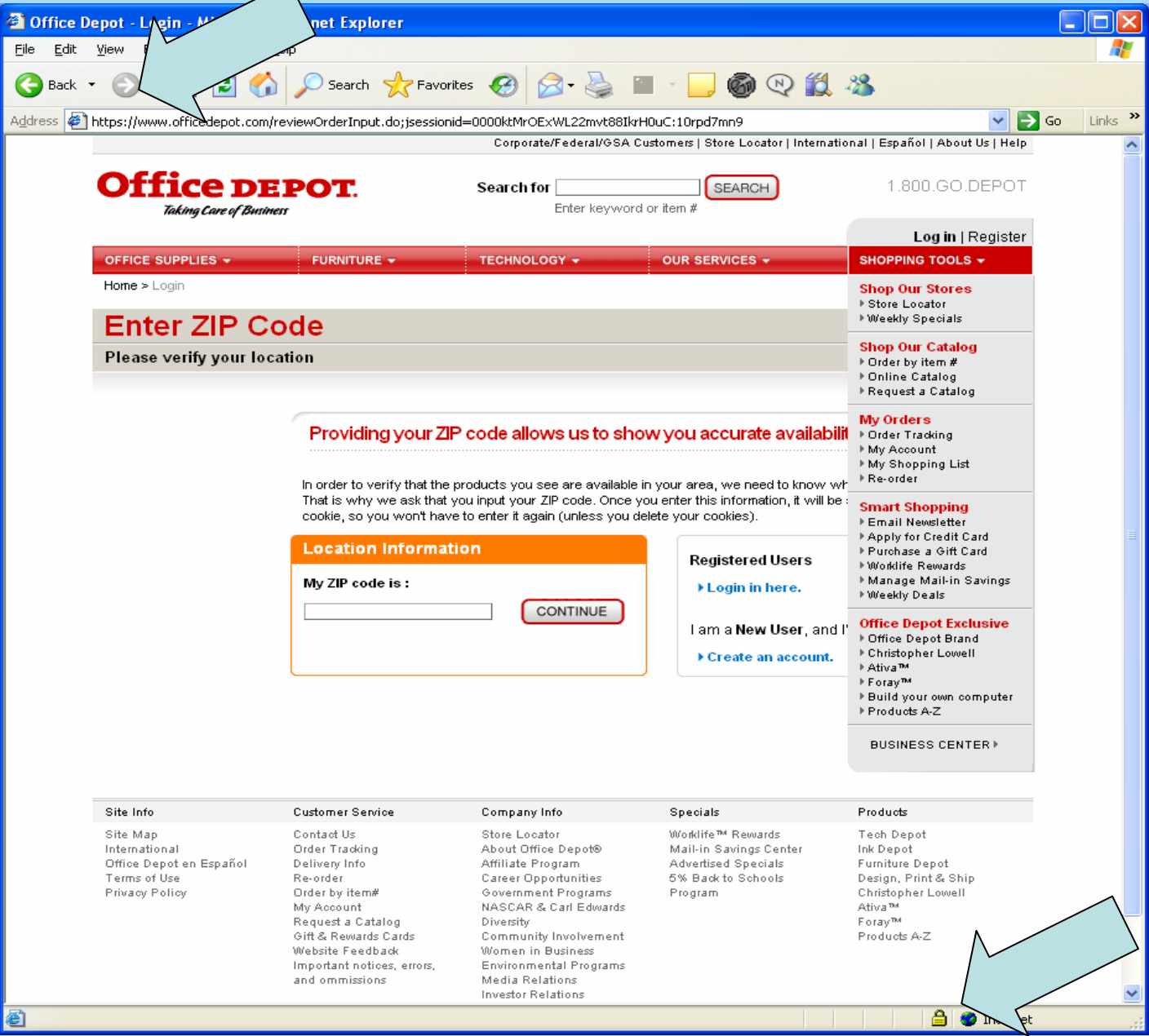


- Verisign (53%)
- Equifax
- Comodo
- Entrust
- CAcert.org (free)

# How to verify transaction is secure

- SSL
- Check Certificate
- Read certificate properties





Search for

1.800.GO.DEPOT

- OFFICE SUPPLIES ▾
- FURNITURE ▾
- TECHNOLOGY ▾
- OUR SERVICES ▾
- SHOPPING TOOLS ▾

Home > Login

## Enter ZIP Code

Please verify your location

### Providing your ZIP code allows us to show you accurate availability

In order to verify that the products you see are available in your area, we need to know what that is why we ask that you input your ZIP code. Once you enter this information, it will be saved as a cookie, so you won't have to enter it again (unless you delete your cookies).

**Location Information**

My ZIP code is :

#### Registered Users

[Login in here.](#)

I am a **New User**, and I

[Create an account.](#)

#### Log in | Register

##### Shop Our Stores

- Store Locator
- Weekly Specials

##### Shop Our Catalog

- Order by item #
- Online Catalog
- Request a Catalog

##### My Orders

- Order Tracking
- My Account
- My Shopping List
- Re-order

##### Smart Shopping

- Email Newsletter
- Apply for Credit Card
- Purchase a Gift Card
- Worklife Rewards
- Manage Mail-in Savings
- Weekly Deals

##### Office Depot Exclusive

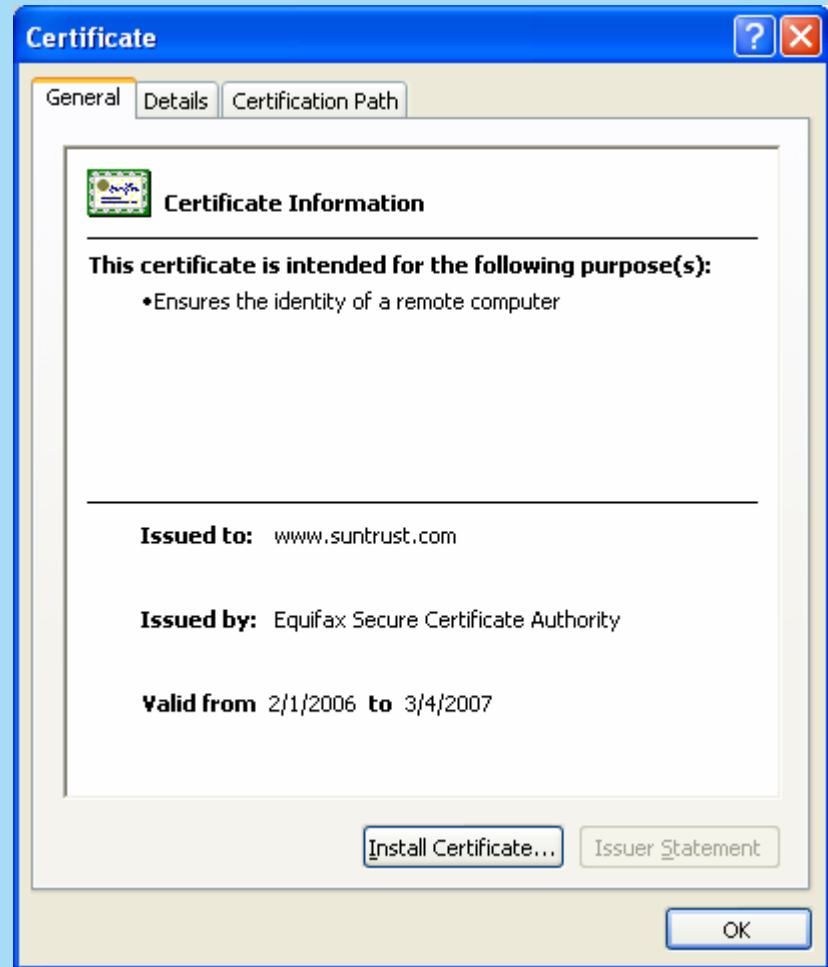
- Office Depot Brand
- Christopher Lowell
- Ativa™
- Foray™
- Build your own computer
- Products A-Z

[BUSINESS CENTER](#) ▶

Site Info	Customer Service	Company Info	Specials	Products
<a href="#">Site Map</a> <a href="#">International</a> <a href="#">Office Depot en Español</a> <a href="#">Terms of Use</a> <a href="#">Privacy Policy</a>	<a href="#">Contact Us</a> <a href="#">Order Tracking</a> <a href="#">Delivery Info</a> <a href="#">Re-order</a> <a href="#">Order by item#</a> <a href="#">My Account</a> <a href="#">Request a Catalog</a> <a href="#">Gift &amp; Rewards Cards</a> <a href="#">Website Feedback</a> <a href="#">Important notices, errors, and omissions</a>	<a href="#">Store Locator</a> <a href="#">About Office Depot®</a> <a href="#">Affiliate Program</a> <a href="#">Career Opportunities</a> <a href="#">Government Programs</a> <a href="#">NASCAR &amp; Carl Edwards</a> <a href="#">Diversity</a> <a href="#">Community Involvement</a> <a href="#">Women in Business</a> <a href="#">Environmental Programs</a> <a href="#">Media Relations</a> <a href="#">Investor Relations</a>	<a href="#">Worklife™ Rewards</a> <a href="#">Mail-in Savings Center</a> <a href="#">Advertised Specials</a> <a href="#">5% Back to Schools Program</a>	<a href="#">Tech Depot</a> <a href="#">Ink Depot</a> <a href="#">Furniture Depot</a> <a href="#">Design, Print &amp; Ship</a> <a href="#">Christopher Lowell</a> <a href="#">Ativa™</a> <a href="#">Foray™</a> <a href="#">Products A-Z</a>

# Reading Certificates

- Issued to:
- Issued by:
- Valid from:



# Questions?

