Table of Contents

• Part 1: Becoming Skilled at Computing
• Part 2: Algorithms and Digitizing Information
• Part 3: Data and Information
  – Chapter 11: Social Implications of IT
  – Chapter 12: Privacy and Digital Security
  – Chapter 13: The Basics of Spreadsheets
  – Chapter 14: Advanced Spreadsheets for Planning
  – Chapter 15: Introduction to Database Concepts
  – Chapter 16: A Case Study in Database Organization
• Part 4: Problem Solving
Learning Objectives

• Explain the meaning of privacy and discuss the issues surrounding privacy of information

• List and explain the meaning of the OECD Fair Information Practices

• Discuss the issues concerning U.S. privacy: Opt-in/Opt-out, compliance/enforcement, coverage

• List the ways a computer can be compromised

• Explain the security methods used in public key cryptosystems (PKCs)

• Perform simple encryption from clear text to cipher text and perform the reverse decryption
Privacy: Whose Information Is It?

• Buying a product at a store generates a transaction, which produces information as follows
  – Paying with cash generally ensures anonymity
  – Paying by check, credit card, or debit card
  – Purchasing through mail order or on the Internet
  – Providing a “preferred customer” number
  – Buying a product that must be registered for a service agreement or warranty

• Who is the owner of the above information?
• How the above information will be used later?
How Can the Information Be Used?

• Transaction information is a normal part of conducting business (keeping a record until our check clears)
  – The transaction information belongs, then, to the store

• If the store decides, based on your previous purchases, to send you ads for other items, the store is using the information for the standard business practice of generating more business

• If the store sells your name to others, has the information been misused?
  – Those other businesses are only trying to generate more business
  – Is it misused if the information gets to the newspaper and is published?
  – Has the store broken the law?
Controlling the Use of Information

• Who controls the use, if any, of the transaction information?

• There are 4 main possibilities:

  1. No Uses: The information ought to be deleted when the store is finished with it
  2. Approval or Opt-in: The store can use it for other purposes, but only if you approve
  3. Objection or Opt-out: The store can use it for other purposes, but not if you object
  4. No Limits: The information can be used any way the store chooses
  5. Internal Use:

      • The store can use the information to conduct business with you (keeping your address, for example), but for no other use
      • It would not include giving or selling your information to another person or business, but it may not require your approval either
Modern Devices and Privacy

• In the past, it was hard for people’s privacy to be violated without their knowledge
• With modern technological devices, people’s privacy can be violated without their knowing it
• Your image and your information deserves “sufficient safeguards against improper circulation”
• If the transaction took place outside the US, the law and standards would place it between (1) and (2) on the spectrum, but very close to (1).
• If the transaction occurred in the US, the law and standards would place it between (3) and (4) on the spectrum, but very close to (4)
• Many Americans assume that there is a privacy law that is close to the fifth case, internal use
A Privacy Definition

- **Privacy**: The right of people to choose freely **under what circumstances and to what extent** they will reveal themselves, their attitude, and their behavior to others.

- Generally, privacy concerns **4 aspects of our lives**: our bodies, territory, personal information, and communication
  - It is the person who decides the circumstances and the extent to which information is revealed, not anyone else
  - The range of features over which the person controls the information embodies **every aspect of the person** — themselves, their attitudes, and their behaviors

- **Enjoying the Benefits of Privacy**
  - Sometimes we want publicity, sometimes we don’t
  - Strong privacy laws insure that we control the dissemination of our information
Threats to Privacy

• What are the threats to privacy?
  – Government
  – Business
  – (Snooping or gossiping private parties, will be handled by security)

• Historically, the governmental threat of spying on its citizens, worries people the most

• The business threat is a more recent worry
  – Surveillance of employees
  – The use of business-related information for other purposes
Voluntary Disclosure

• In principle, a person can enjoy perfect privacy by simply deciding not to reveal anything to anyone

• It may be in our interest to reveal private information, freely in exchange for real benefits
  – Doctors receive our personal information so they can help us stay healthy
  – Credit card companies get our personal information to check our credit record in exchange for the convenience of paying with a card
  – Employers read our email at work, because we are using the employer’s computer for a job
  – The government may have information on us regarding our parents' names and birthplaces, our race and ethnicity, etc. for the purpose of enjoying the rights of citizenship

• How private can we be when we reveal so much about ourselves, our attitudes, and our behavior?
Fair Information Practices

- If people or organizations are free to give or sell the information to anyone else, our privacy is compromised ➔ **There must be clear guidelines**

<table>
<thead>
<tr>
<th>Table 12.1</th>
<th>A brief explanation of the OECD’s Fair Information Practices Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limited Collection</strong></td>
<td>There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.</td>
</tr>
<tr>
<td><strong>Purpose</strong></td>
<td>The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.</td>
</tr>
<tr>
<td><strong>Quality</strong></td>
<td>The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td><strong>Use Limitation</strong></td>
<td>Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.</td>
</tr>
<tr>
<td><strong>Openness</strong></td>
<td>There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.</td>
</tr>
<tr>
<td><strong>Participation</strong></td>
<td>An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.</td>
</tr>
<tr>
<td><strong>Accountability</strong></td>
<td>The data controller should be accountable for complying with these principles.</td>
</tr>
</tbody>
</table>
OECD Fair Information Practices

• By Organization for Economic Cooperation and Development (OECD) in 1980
  – They have become a widely accepted standard
  – The public has an interest in these principles becoming law

• The principles also give a standard that businesses and governments can meet as a “due diligence test” for protecting citizens’ rights of privacy, thereby protecting themselves from criticism or legal action

• An important aspect of the OECD principles is the concept that the data controller (the person or office setting the policies) must interact with individuals about their information, if any, and must be accountable for those policies and actions!
Privacy Worldwide

• Privacy is not enjoyed in much of the world
• Privacy often conflicts with the goals of businesses and governments:
  – Example, the United States has not adopted the OECD principles, possible because many U.S. companies profit by buying and using information in ways that are inconsistent with the OECD principles
• The European Union (EU) issued a benchmark law incorporating the OECD principles
  – EU Directive requires that data about EU citizens be protected by the standards of the law even when it leaves their country
• Other countries adopted it as well including Australia, Canada, Hong Kong, and New Zealand
Figure 12.1 Comparison of privacy and data protections by country.
Business as Usual

- US businesses and government gathers data contrary to the OECD rules
- US Patriot Act makes it a crime to say that data gathering is taking place
- Almost every store and company you do business with has information about you
  - if you want to know what they are doing with that information you must read their privacy policies
  - often it says, “We use the information however we like.”
Targeted by “Target”

• **Data Mining** (known as “Big Data”) is the statistical analysis of huge information archives

• The retailer “Target”
  – Assigns each stopper a unique code
  – **Records various things**: credit card usage, coupon usage, online survey, mails in refund, calls to the customer help line, Target website visits, …

• Figure out if a woman is pregnant from her buying habits
  – Develop a list of “about 25 products that, when analyzed together, allow then assign each shopper a pregnancy prediction score”
Government, as Usual

- In June 2013, Edward Snowden, an analyst for US NSA (National Security Agency) revealed as followings
- The U.S. government was collecting complete metadata records from telephone carriers, including data to calls to other countries with OECD laws in place
- The government was also collecting online activity from Facebook, Microsoft, Google, etc. using a surveillance program called PRISM
- It is still unknown if these allegations (주장, 탄원) are true
- US NSA claims that the justification for the collection is the US Patriot Act of 2001
Tracking

- In electronic privacy, tracking is used in 2 different ways
  - **online tracking**: Web site automatically sending details about your visit to other content providers (to show you adds and other products)
  - **cell phone tracking**: positioning information, used to map your physical location

**Online Tracking**

- We assume it is used to target advertising and marketing organizations
- But anyone could arrange to follow your “click streams”
- HTTP has a “Do Not Track” flag that tells Web servers your tracking preferences
  - It is up to the Web server to honor your request
**Notice that Google’s Chrome browser does **not** support **user requests not to track**.

- “Do Not Track” is controversial because consumer behavior is very valuable, but people don’t want anyone following them around (even online)
Even More Private!

- **Industry Initiatives**
  - National Advertising Initiative (NAI) opt-out program: (http://www.networkadvertising.org/choices/)
  - Digital Advertising Alliance: (www.aboutads.info/choices)

- **Privacy Initiatives**
  - Abine.com offers a free blocker DoNotTrackMe: https://www.abine.com/index.php

- **Private Browsing** (IE’s InPrivate, FireFox’s PrivateBrowsing, Chrome’s Incognito)
  - The “client side” facility which only concerns the information stored locally on your machine, not what's stored on servers
  - All cookies, cached files, and history are deleted at the end of the session
  - Useful when using a public computer
# Cell Phones

- Even if GPS is off, the location of a cell phone can be detected, based on proximity to cell phone towers.
- Freedom of Information Act (FOIA) request was launched in 2010.
  - 정보공개법: 국정운영의 투명성확보를 위해 공공기관의 정보는 국민이 요구하면 공개한다
  - Companies keep it for a while, and the NSA keeps it permanently.

<table>
<thead>
<tr>
<th></th>
<th>Verizon</th>
<th>T-Mobile</th>
<th>AT&amp;T/Cingular</th>
<th>Sprint</th>
<th>Nextel</th>
<th>Virgin Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Information</td>
<td>Post-paid: 3–5 years</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Call detail records</td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Pre-paid: varies</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>2 years</td>
</tr>
<tr>
<td>Cell towers used by phone</td>
<td>1 rolling year</td>
<td>Officially 4–6 months, really a year or more.</td>
<td>From July 2008</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>Not retained — obtain through Sprint</td>
</tr>
<tr>
<td>Text message detail</td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Post paid: 5–7 years</td>
<td>18 months (depends on device)</td>
<td>18 months (depends on device)</td>
<td>60–90 days</td>
</tr>
<tr>
<td>Text message content</td>
<td>3–5 days</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
</tr>
<tr>
<td>Pictures</td>
<td>Only if uploaded to Web site (customer can add or delete pictures any time)</td>
<td>Can be stored online and are retained until deleted or service is canceled</td>
<td>Not retained</td>
<td>Contact provider</td>
<td>Contact provider</td>
<td>Not retained</td>
</tr>
<tr>
<td>IP session information</td>
<td>1 rolling year</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td>IP destination information</td>
<td>90 days</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td>Bill copies (post-paid only)</td>
<td>3–5 years, but only last 12 months readily available</td>
<td>Not retained</td>
<td>5–7 years</td>
<td>7 years</td>
<td>7 years</td>
<td>n/a</td>
</tr>
<tr>
<td>Payment history (post-paid only)</td>
<td>3–5 years, check copies for 6 months</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>n/a</td>
</tr>
<tr>
<td>Store Surveillance Videos</td>
<td>Typically 30 days</td>
<td>2 weeks</td>
<td>Depends. Most stores carry for 1–2 months</td>
<td>Depends</td>
<td>Depends</td>
<td>n/a</td>
</tr>
<tr>
<td>Service Applications</td>
<td>Post-paid: 3–5 years</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Depends</td>
<td>Depends</td>
<td>Not retained</td>
</tr>
</tbody>
</table>

Figure 12.2 Retention periods for information held by cellular phone providers.
Cookies: Appearing to stay connected [1/2]

• In client/server environment, the server is helping many clients at once
• In order to know who’s who, the server stores a cookie of information (7 field)
  • That uniquely identifies the identity of a client across a series of independent client/server events (originally by Netscape engineers)
• Cookies are exchanged between the client and the server on each transmission of information

www.nasm.si.edu  FALSE / FALSE  2052246450  CFTOKEN  89367880

• The first is the server and the last is the unique information identifying the session
Cookie Abuse

- A cookie is exchanged between the client and server making the interaction private
- There is a loophole called a third-party cookie
  - If the Web site includes ads on its page, the server may direct it to link to the advertising company to deliver the ad
  - This new client/server relationship places a cookie on your computer
- All browsers allow users to control how cookies are processed
  - You could turn them off, forcing the browser to ask you every time whether you will accept a cookie or not
  - Turning off cookies prevents you from being able to bank online
- Simply set your browser’s cookie policy to your own comfort level
Tracking

- [ ] Tell websites I do not want to be tracked

History

Firefox will: [ ] Use custom settings for history

- [ ] Always use private browsing mode
- [ ] Remember my browsing history
- [ ] Remember download history
- [ ] Remember search and form history
- [ ] Accept cookies from sites
  - [ ] Accept third-party cookies
    - Keep until: [ ] they expire
- [ ] Clear history when Firefox closes

Location Bar

When using the location bar, suggest: [ ] Bookmarks
The Right to Be Forgotten

- **Scenario**: One day in a Connecticut internet newspaper headline….
- A nurse with a clean police record is arrested for carrying a small amount of marijuana.
- In 2 days, she was freed and her case was dismissed because it was her first offense, and she agreed to go to drug counseling.
- From the legal point of view, it is as if the arrest never happened according to the law.
- But…
- Later she cannot be hired because of the internet newspaper headline.
- **Clean legal record!, but the public record “internet newspaper” is not clean!**
- **Some mechanism is need for the right to be forgotten**
  - A particular flag which can inform the search engine to go around the article.
Identity Theft

• The Security Principle of the Fair Information Practices is also important
  – Those who hold private information are obligated to maintain its privacy against unauthorized access and other hazards

• How can this private information be used?
  – One possibility is identity theft which is the crime of posing as someone else for fraudulent purposes

• ChoicePoint Case (Feb 2005) announced that their personal data of 145,000 are viewed by unauthorized parties
  – But it turned out that ChoicePoint sold the personal data to identity thieves
  – Over 800 identity thefts have been reported from this case
  – The Federal Trade Commission ordered $10 million civil fines and $5 million consumer redress
Digital Security

• Computer security is a topic that is in the news almost daily

• Remember the long list of “dos and don’ts” for online behavior?
  – Do check with the sender before opening an attachment you’re unsure about
  – Don’t fall for phishing emails
  – And the other’s from Chapter 11?

• The Risks: What can happen?
  – Mischief: infecting a computer, causing a nuisance, erasing files, trashing files, …
  – Information theft: stealing personal information
  – Spying: surreptitiously recording videos of the user, logging keystrokes, compromising secure online activities
  – Resource theft: taking over a computer (making it a “zombie”)
Terms and Jargon

- **Malware**: software that harms computers
- **Virus**: shared program that contains code to reproduce itself
- **Worm**: program that is often embedded in an email attachment, reproduces itself and sends a copy to everyone on your contact list
- **Exploit**: Malicious software takes advantage of bugs in commercial software for penetrating an entry point
- **Trojan**: an unasked-for gift that is a malicious program that performs unauthorized activities

**Bad Behaviors**

- **Backdoors**: SW that creates an access path allowing attackers to run any program on your computer
- **Trojans**: SW that may record every key you type (trying to find passwords), extort money, watch for banking and credit card information
- **Rootkits**: SW that infects your computer and then fights back against security systems
Table 12.2 Results for search terms from Myhrvold's "Free Stuff" experiment.

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Results</th>
<th>Infected Files</th>
<th>Threats Detected by Lavasoft Ad-Aware</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;free wallpaper&quot;</td>
<td>2/6</td>
<td>11</td>
<td>Adware, Adware Installer, unwanted programs, miscellaneous</td>
</tr>
<tr>
<td>&quot;free screensaver&quot;</td>
<td>8/10</td>
<td>191</td>
<td>Hijacker, Adware, Adware Installer, unwanted programs, cookies, miscellaneous</td>
</tr>
<tr>
<td>&quot;free games&quot;</td>
<td>2/10</td>
<td>45</td>
<td>Adware, Adware Installer, cookies</td>
</tr>
<tr>
<td>&quot;free game cheats&quot;</td>
<td>0/1</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>&quot;free word unscrambler&quot;</td>
<td>0/10</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>&quot;free e-cards&quot;</td>
<td>0/10</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>&quot;free lyrics&quot;</td>
<td>5/10</td>
<td>608</td>
<td>Adware, Adware Installer, toolbar, cookies</td>
</tr>
<tr>
<td>&quot;free music downloads&quot;</td>
<td>5/10</td>
<td>835</td>
<td>Trojan, Adware, Adware Installer, toolbar, browser, plug-in, miscellaneous</td>
</tr>
</tbody>
</table>
Safe Computing Checklist

- Turn off Bluetooth when not in use
- Keep your phone and other computers locked
- Do not automatically click on email attachments
- Never enter sensitive information in a pop-up
- Thinking of getting something for nothing… Think again
- Know where you’re going
- Be somewhat skeptical
- Use extreme care when visiting notorious sites
Table 12.3 File extensions that can carry malware, primarily for Windows OS. (Recall that the file extension is the letter sequence following the last dot in the file name.)

<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.386</td>
<td>Virtual Device Driver (Windows 386 enhanced mode)</td>
</tr>
<tr>
<td>.3gr</td>
<td>VGA Graphics Driver/configuration files</td>
</tr>
<tr>
<td>.add</td>
<td>Adapter Driver file</td>
</tr>
<tr>
<td>.ade</td>
<td>Microsoft Access project extension</td>
</tr>
<tr>
<td>.asp</td>
<td>Active Server Page</td>
</tr>
<tr>
<td>.bas</td>
<td>Microsoft Visual Basic class module</td>
</tr>
<tr>
<td>.bat</td>
<td>Batch file</td>
</tr>
<tr>
<td>.chm</td>
<td>Compiled HTML Help file</td>
</tr>
<tr>
<td>.cmd</td>
<td>Microsoft Windows NT command script</td>
</tr>
<tr>
<td>.com</td>
<td>Microsoft MS-DOS program</td>
</tr>
<tr>
<td>.cpl</td>
<td>Control Panel extension</td>
</tr>
<tr>
<td>.crt</td>
<td>Security certificate</td>
</tr>
<tr>
<td>.dbx</td>
<td>Database Index</td>
</tr>
<tr>
<td>.dll</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>.exe</td>
<td>Program file</td>
</tr>
<tr>
<td>.fon</td>
<td>Font file</td>
</tr>
<tr>
<td>.hlp</td>
<td>Help file</td>
</tr>
<tr>
<td>.hta</td>
<td>HTML program</td>
</tr>
<tr>
<td>.inf</td>
<td>Setup information</td>
</tr>
<tr>
<td>.ins</td>
<td>Internet Naming Service</td>
</tr>
<tr>
<td>.isp</td>
<td>Internet communication settings</td>
</tr>
<tr>
<td>.js</td>
<td>JavaScript file</td>
</tr>
<tr>
<td>.jse</td>
<td>JavaScript encoded-script file</td>
</tr>
<tr>
<td>.ink</td>
<td>Shortcut</td>
</tr>
<tr>
<td>.mdb</td>
<td>Microsoft Access program</td>
</tr>
<tr>
<td>.mde</td>
<td>Microsoft Access MDE database</td>
</tr>
<tr>
<td>.msc</td>
<td>Microsoft Common Console document</td>
</tr>
<tr>
<td>.msi</td>
<td>Microsoft Windows Installer package</td>
</tr>
<tr>
<td>.msp</td>
<td>Microsoft Windows Installer patch</td>
</tr>
<tr>
<td>.mst</td>
<td>Microsoft Windows Installer Transform file</td>
</tr>
<tr>
<td>.ocx</td>
<td>Microsoft Object Linking</td>
</tr>
<tr>
<td>.pcd</td>
<td>Corel Adaptec CD Creator image file</td>
</tr>
<tr>
<td>.pif</td>
<td>Shortcut to MS-DOS program</td>
</tr>
<tr>
<td>.reg</td>
<td>Registration entries</td>
</tr>
<tr>
<td>.scr</td>
<td>Screen saver</td>
</tr>
<tr>
<td>.sct</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.shb</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.shs</td>
<td>Shell Scrap object</td>
</tr>
<tr>
<td>.url</td>
<td>Internet shortcut</td>
</tr>
<tr>
<td>.vb</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vbe</td>
<td>Visual Basic Script-encoded file</td>
</tr>
<tr>
<td>.vbs</td>
<td>Visual Basic Script file</td>
</tr>
<tr>
<td>.vxd</td>
<td>Microsoft Windows Virtual Device Driver</td>
</tr>
<tr>
<td>.wsc</td>
<td>Windows Script Component</td>
</tr>
<tr>
<td>.wsf</td>
<td>Windows Script File</td>
</tr>
<tr>
<td>.wsh</td>
<td>Windows Script Host Settings file</td>
</tr>
</tbody>
</table>
Oops, Now I’ve Done it!

- If Something Really Bad Happens
  - Turn off your computer immediately
  - Use a different computer to do a web search about what happened
  - Use an external source for the OS to reboot

Plan of Action

- Run “modern” software & Install updates often
- Install anti-virus software
- Set your Wi-Fi router to security level of at least WPA2
- Protect your phones and computers with appropriate passwords
- Use your knowledge, be wise
Encryption for Transmitting Documents Safely

• Information that is recoded to hide its true meaning uses encryption

• The key is a “magic number” used to transform (encrypt) text (clear text) into gibberish (cipher text): Private Key vs Public Key

• Both the sender and receiver must agree on the key

• Here we study 2-way cipher for transmitting secure documents!

• Remember the 1-way cipher for computer password!
  – You set up a password and the system saves the encrypted key
  – Nobody but you knows the password, even the system does not know it
  – If you lose it, the process for setting a new password is initiated
Private Key Encryption

• 5-Step Encryption algorithm:
  – The sender breaks the message into groups of letters
  – The sender “multiplies” each group of letters by the key
  – Send the “products” (results from the “multiplications”) to the receiver
  – The receiver “divides” the “products” by the key to recreate the groups
  – Assemble the groups into the message

• The “reversibility” of encryption makes them 2-way ciphers
  – Only the sender and receiver know the key, making the products useless numbers

• The technique just explained is called private key encryption, or symmetric-key cryptography
1. Break into groups, say, ME ET b@ b9. (The blank is a letter, too; I have coded as b.) These letters are, when the ASCII is converted to decimal: 7769 6984 3264 3257.

2. “Multiply” each group by the key, 13:
- $7769 \times 13 = 100997$
- $6984 \times 13 = 90792$
- $3264 \times 13 = 42432$
- $3257 \times 13 = 42341$

(The “first zeroes” make all number six digits.)

3. Send the “products” 100997 090792 042432 042341 to the receiver.

4. The receiver “divides” by the key, 13:
- $100997/13 = 7769$
- $090792/13 = 6984$
- $042432/13 = 3264$
- $042341/13 = 3257$

producing numbers mapped by ASCII: ME ET b@ b9

5. Reassembling the message, MEET @ 9.

---

**Figure 12.4** Schematic diagram of a cryptosystem. Using a key $K_{SR}$ known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext. In the middle, where the content is exposed and can be snooped here.
Beyond Private Key Encryption

• Real encryption systems use much longer blocks (hundreds of letters) and larger keys

• Multiplication, division are not the only operations that can be used for encryption

• All that is needed is for an operation to have an inverse (divide is the inverse of multiply)

• Private key encryption works very well.. But…
  
  – The sender and receiver have to agree on the key, so they should meet face-to-face

• To avoid that face-to-face meeting, publish the key! ➔ Public Key!

• The public key encryption uses 2 special prime numbers multiplied together
Public Key Encryption Steps

- After, the receiver publishes the special key, K, the following happens:
  - The sender breaks up the message into blocks as before
  - The sender cubes each block, divides by K, and transmits only the remainders
  - The receiver raises each remainder to a high power determined by the prime numbers and known only to him
  - The receiver divides by K, too, and saves only the remainders, which are the original blocks.
  - The receiver assembles the message

![Diagram](image)

**Figure 12.5** Public key cryptosystem. The sender uses the receiver’s public key $K_R$ to encrypt the cleartext, and only the receiver is able to decrypt it to recover the cleartext.
How Do We Know It Works?

• K, the magic public key, is just 2 prime numbers, p and q, multiplied together
• It is possible to figure out those 2 numbers from the published key in theory
• This process, called factoring, is tough if the numbers p and q are large (60 digits apiece)
• It is impractical to factor them no matter how powerful the computer!

• Contributors
  – Leonard Euler: Prime Number
  – Whitefield Diffie and Martin Hellman: 2 prime numbers and cubing
  – Ron Rivest, Adi Shamir, Len Adleman: PKC Algorithm, called RSA
Encryption

• We encrypt (encode) our data so others can’t understand it (easily) except for the person who is supposed to receive it.

• We call the data to encode plaintext and the encoded data the ciphertext.

• Encoding and decoding are inverse functions of each other.
Encryption/decryption

secret key → Encryption algorithm → ciphertext

plaintext → Encryption algorithm → ciphertext

secret key → Decryption algorithm → ATTACKATDAWN

ATTACKATDAWN → Encryption algorithm → AGSTEMENDO

ATTACKATDAWN → Decryption algorithm → plaintext
Cryptanalysis

secret key

Encryption algorithm

Ciphertext

plaintext

Mathematical, logical, empirical analysis

 ATTACKATDAWN

ATTACKATDAWN

15110 Principles of Computing, Carnegie Mellon University
Two basic ways of altering text to encrypt/decrypt

- Substitute one letter for another using some kind of rule
  - Substitution cipher
- Scramble the order of the letters using some kind of rule
  - Transposition cipher
Substitution Ciphers

• Simple encryption scheme using a substitution cipher:
  ○ Shift every letter forward by 1:
    A → B, B → C, ..., Z → A

• Example:
  MESSAGE → NFTTBHF

• Can you decrypt TFDSFU?
Caesar Cipher

- Shift forward \( n \) letters; \( n \) is the secret key
- For example, shift forward 3 letters:
  \[A \rightarrow D, \ B \rightarrow E, \ldots, \ Z \rightarrow C\]
  - This is a Caesar cipher using a key of 3.
- MESSAGE \( \rightarrow \) PHVVDJH
- How can we crack this encrypted message if we don’t know the key?
  DEEDUSEKBTFEIIYRBOTUSETUJXYI
Transposition ciphers

an ancient Greek method

STSF...EROL...NOUA...DOTN...MPHK...OSEA...RTRN...EOND...
Encryption in computing

Symmetric vs. asymmetric encryption

- **Symmetric** (shared-key) encryption: commonly used for long messages
  - Often a complicated mix of substitution and transposition encipherment
  - Reasonably fast to compute
  - Requires a shared secret key usually communicated using (slower) asymmetric encryption

- **Asymmetric** encryption: different keys are used to encrypt and to decrypt
Keypspace

- *Keypspace* is jargon for the number of possible secret keys, for a particular encryption/decryption algorithm

- Number of bits per key determines *size of keyspace*
  - important because we want to make *brute force attacks* infeasible
  - brute force attack: run the (known) decryption algorithm repeatedly with every possible key until a sensible plaintext appears

- Typical key sizes: several hundred bits
Symmetric (Shared Key) Encryption

Ciphertext = Enc(plaintext, key)

Alice

Encrypt using key

Plaintext

Alice uses the shared key to encrypt the plaintext to produce the ciphertext

Bob

Decrypt using key

Plaintext = Dec(Ciphertext, key)

Bob uses the shared key to decrypt the ciphertext to recover the plaintext

Enc() and Dec() are functions
Establishing Shared Keys

- Problem: how can Alice and Bob secretly agree on a key, using a public communication system?

- Solution: asymmetric encryption based on *number theory*
  - Alice has one secret, Bob has a different secret; working together they establish a shared secret
  - Examples: Diffie-Hellman key exchange, RSA public key encryption
One type of asymmetric encryption: RSA

- Common encryption technique for transmitting symmetric keys on the Internet (https, ssl/tls)
  - Named after its inventors: Rivest, Shamir and Adleman
  - Used in https (you know when you’re using it because you see the URL in the address bar begins with https://)
Asymmetric Public Key Encryption

- Alice uses Bob’s public key to encrypt the plaintext to produce the ciphertext.
- Bob uses his private key to decrypt the ciphertext to recover the plaintext.

\[
ciphertext = Enc(plaintext, \text{pubB})
\]

\[
plaintext = Dec(ciphertext, \text{privB})
\]
How RSA works

- First, we must be able to represent any message as a single number (it may already be a number as is usual for a symmetric key)
- For example:

\[
\text{ATTACKATDAWN} \\
012020010311012004012314
\]

Public and Private Keys

- Every receiver has a public key \((e, n)\) and a private key \((d, n)\).
- The transmitter encrypts a (numerical) message \(M\) into ciphertext \(C\) using the receiver’s public key:

\[
M^e \text{ modulo } n \rightarrow C \quad (\text{ciphertext})
\]

- The receiver decodes the encrypted message \(C\) to get the original message \(M\) using the private key (which no one else knows):

\[
C^d \text{ modulo } n \rightarrow M \quad (\text{plaintext})
\]
RSA Example

- Alice’s Public Key: (3, 33)  \( (e = 3, n = 33) \)
- Alice’s Private Key: (7, 33)  \( (d = 7, n = 33) \)
  - Usually these are really huge numbers with many hundreds of digits!

- Bob wants to send the message 4
  - Bob encrypts the message using \( e \) and \( n \):
    \[ 4^3 \mod 33 \rightarrow 31 \]
    ... Bob sends 31

- Alice receives the encoded message 31
  - Alice decrypts the message using \( d \) and \( n \):
    \[ 31^7 \mod 33 \rightarrow 4 \]
Generating $n$, $e$ and $d$

- $p$ and $q$ are (big) random primes.
- $n = p \times q$
- $\varphi = (p - 1)(q - 1)$
- $e$ is small and relatively prime to $\varphi$
- $d$, such that:
  
  \[ e \times d \mod \varphi = 1 \]

\[ p = 3, \quad q = 11 \]
\[ n = 3 \times 11 = 33 \]
\[ \varphi = 2 \times 10 = 20 \]
\[ e = 3 \]
\[ 3 \times d \mod 20 = 1 \]
\[ d = 7 \]

Usually the primes are huge numbers--hundreds of digits long.

e, n 값은 알려진것이고 $p, q$만 알아내면, $\varphi$ 을 알고 그러면 $d$값을 알아낼수 있다!, But…………
Cracking RSA

- Everyone knows \((e, n)\). Only Alice knows \(d\).
- If we know \(e\) and \(n\), can we figure out \(d\)?
  - If so, we can read secret messages to Alice.
- We can determine \(d\) from \(e\) and \(n\).
  - Factor \(n\) into \(p\) and \(q\).
    \[ n = p \times q \]
    \[ \varphi = (p - 1)(q - 1) \]
    \[ e \times d = 1 \pmod{\varphi} \]
  - We know \(e\) (which is public), so we can solve for \(d\).
- But **only** if we can factor \(n\)
RSA is safe (for now)

- Suppose someone can factor my 5-digit $n$ in 1 ms,

- At this rate, to factor a 10-digit number would take 2 minutes.
- ... to factor a 15-digit number would take 4 months.
- ... 20-digit number... 30,000 years.
- ... 25-digit number... 3 billion years.

- We're safe with RSA! (at least, from factoring with digital computers)
Certificate Authorities

- How do we know we have the right public key for someone?
- Certificate Authorities sign digital certificates indicating authenticity of a sender who they have checked out in the real world.
- Senders provide copies of their certificates along with their message or software.
- But can we trust the certificate authorities? (only some)
Redundancy Is Very, Very, Very Good

• Take precautions with your technology!
• Businesses archive files daily and store these backups off-site
• They have a system recovery team to clean up after a disaster strikes
• They also have system redundancy: multiple computers performing the same work, so that when one fails, another is up and running

• Individual users also should prepare for the personal disasters of your computing environment
  – Losing your notebook in the student union
  – The hard disc of your PC is broken at some point
2-Step Recovery Program

- Full backup
  - A complete copy of everything written on the system as of a date and time

- Partial backup
  - Changes since the last full (or partial) backup are saved
  - IE. keep a copy of any files or folders that have been created or modified

- After a disaster, recover files as follows
  - Install the last full backup copy
  - Then make the changes saved in the partial backups in order
  - Continue with each partial backup until the most recent
  - That's as close to "full recovery" as possible

- Commercial Back-Up System vs Personal Back-Up
Backing Up a Personal Computer

• First, you need a place to keep the copy, and you need software to make the copy
  – “In an external hard disk” or “in the cloud”

• The “cloud” company’s computers store the information for you and they take responsibility of keeping it available to you

• You don’t have to back up the following:
  – Information that can be recreated from some permanent source
  – Information that was saved but that has not changed
  – Information that you don’t care about
Recovering Deleted Information

- If you accidentally delete important files, file restoration (that backup copy!) is your savior!

- Backups are useful for your personal computing activity
- Backups can even be used for saving evidence of crimes or inappropriate behavior
- Two copies of email are produced immediately when the Send button is clicked— one in the sent mail directory, and one somewhere else

- It can be difficult to eradicate all copies of digital information!
- Modern-day is the age of trace!
• Revealing personal information can be beneficial, so the people and organizations that receive the information must keep it private
  – The OECD guidelines for keeping data private

• Guidelines often conflict with the interests of business and government, so some countries like the United States have not adopted them
  – Because the United States takes a sectorial approach to privacy, adopting laws only for specific business sectors or practices, much of the information collected on its citizens is not protected by OECD standards

• DoNotTrackMe should be installed to avoid third parties building a profile of your Web surfing behavior

• The best way to manage privacy in the Information Age is to have OECD-grade privacy laws
Summary [2/2]

- Public key cryptography (PKC) is a straightforward idea built on familiar concepts: private key encryption vs public key encryption.
- Computer scientists have not yet proved the invincibility of the RSA scheme, but it can be “made more secure” simply by increasing the size of the key.
- Viruses and worms cause damage:
  - We can reduce the chance of infection by installing and running anti-virus SW.
  - We must be aware of hoaxes and phishing scams.
- We can implement a plan of action to ensure that our personal computers remain private and secure.
- Backing up computer files is an essential safeguard.