Chapter 2
ACCOUNTING ON THE INTERNET

Discussion Questions

2-1. An intranet is an internal network created by an organization for the benefit of its employees. Most intranets are local area networks that utilize convenient web-browsing software. Extranets are similar to intranets, except that they are also accessible by a limited number of external parties—for example, employees working from home or suppliers.

Both intranets and extranets are valuable to accountants. For example, intranets enable businesses to distribute, and end users to read, information about such items as production reports, announcements, or financial activities. They also enable accountants to collaborate with each other, using group collaboration tools. These same ideas apply to extranets. Finally, these networks are important to accountants because so much commerce and financial information is transmitted over them and also because their security and efficiency are important auditing concerns.

2-2. The term "blogs" is an abbreviation for *web logs*, and is a groupware (collaboration) tool that allows computer users and web browsers to publish personal messages online. Blogs enable their users to create, share, and leverage knowledge in any kind of organization. Those who are currently exploring the potential of blogs are for-profit companies, government organizations, and universities.

2-3. As of June, 2014, Bitcoin was still a viable currency that was trading at $444.80 (U.S. dollars) per coin. Every other virtual currency has eventually failed, however, so checking the price daily might be important to owners. This question also asks students whether they would buy bitcoins. Their answers can create some lively class discussion.

2-4. Commentary on social media sites such as Facebook or Twitter also contains useful information to businesses. For example, an automobile manufacturer might check such sites to gauge public reaction to a recent safety recall, a fast-food chain might check them to measure public opinion about a new meal offering, or a music figure might check them to assess whether a new record album has created enough "buzz."

According to a recent survey of 2,100 companies by researchers at Harvard University, nearly 80% of survey respondents use, or plan to use, social media for business purposes, while 69% anticipate expanded use of such resources in the future. Again according to this survey, about half of all businesses plan to use it to increase public awareness of their organizations, products, or services—an application of perhaps special interest to public accounting firms.

2-5. *Hypertext markup language (html)* is a computer programming language that enables users to create web pages for use on the Internet. Most of the web pages that we

view on the Internet employ it. If you use Microsoft Internet Explorer, you can view the source code for a given web page by selecting "Source" from the View menu.

HTML is mostly an editing language that tells a web browser how to display the contents of a web page. But HTML tags cannot be changed or customized. To solve this problem, developers have extended HTML with *XML*—an acronym for "extensible markup language" that allows users to create their own tags. Anyone can create such tags, but businesses need standards. For example, we don't want one entity using <SalesRevenues> while another uses <Sales>. One XML standard is XBRL—an acronym for "extensible business reporting language." As noted in the text, the XBRL International Consortium develops international standards for this language.

2-6. As explained in question 5 above, XBRL is a standardized subset of XML. Businesses can use the documents created and saved in XBRL format in many different ways without having to re-key the data—a very real advantage. Until recently, however, most government agencies stored the data submitted to them by individuals or businesses in either hard-copy formats or word documents. Today, however, government agencies are also storing such data in XBRL formats. One such agency is the Securities and Exchange Commission (SEC), which stores corporate financial data such as 10-k reports in a database called IDEA—an acronym for "Interactive Data and Electronic Applications." The relationship between XBRL and IDEA is very direct, therefore: IDEA is a database containing XBRL-coded, financial information.

2-7. *Electronic commerce (EC)* means conducting business electronically. Examples of electronic commerce include retail sales over the Internet and EDI (the ability to electronically transmit such documents as invoices, credit memos, purchase orders, bids for jobs, and payment remittance forms). Much EC is performed over the Internet, but companies such as Wal-Mart, IGT, and some of the phone companies also transmit messages over private networks or communications channels to which the general public does not have access.

EC is important because (1) there is so much of it today, (2) the uses of EC are expanding, (3) even the smallest company can create a website and compete with larger businesses, and (4) Internet retail sales are growing. As noted in the text, some businesses now rely on the Internet for over half of their annual sales revenues. For businesses such as Dell, Amazon.com, or E-trade, the percentage is much larger.

EC is important to accountants because electronic documents can be more difficult to control, authenticate, or audit. Security is also a major issue because assets are less tangible, compromised systems are not obvious, and information losses are not easy to verify. The final section of the chapter discusses some major privacy and security concerns.

2-8. *Electronic payments (E-payments)* are payments that customers make to sellers electronically. They are similar to credit card payments except that they use third parties. It works like this: A customer buys something from a seller, using credit advanced by the third party—e.g., Paypal. The third party pays the seller and then, in turn, debits the buyer's credit

card or account. One advantage of using such a system is that buyers need only provide their credit card numbers or otherwise establish accounts with one company—the e-payment company—not each company with which they wish to do business. Another major justification for using E-payments is *security*. Credit-card information is at risk when it is transmitted over data communications lines or stored in the computer files of many vendors.

2-9. *Electronic data interchange (EDI)* refers to transmitting routine business documents such as shipping notices, customs forms, invoices, and purchase orders electronically. Companies use EDI because it is often a superior way of doing business. For example, because the outputs from one company (e.g., the information on a computerized purchase order) are the inputs to another company, EDI allows its users to avoid the time delays and costs of transcribing the data once the information has been received. This eliminates data-entry bottlenecks and reduces the errors such data transcription typically introduces into an AIS. Other advantages of EDI discussed in the chapter are: (1) streamlining processing tasks, (2) faster response to customer queries or vendor data transmissions, (3) reductions in paperwork, and (4) a secure processing environment that is separate from the post office or an overnight delivery system.

2-10. This question asks students how comfortable they are giving their credit card numbers to retail websites and therefore has no right or wrong answer. While some individuals are comfortable entering their credit card numbers into websites for Internet purchases, others fear for their cards' security. There is certainly much to fear. Identity theft, in which someone steals the identity of another, is easy when the thief knows such important information as a person's credit card number(s) and similar personal information.

2-11. A common way for the owners of one website to charge for advertising from a second party is to charge a set fee (for example, $1) each time a viewer clicks on the advertiser's link(s). But this requires the website administrator to count the actual number of clicks, per month. Click fraud occurs when website personnel repeatedly click on that link themselves or artificially inflate their counts, thereby defrauding the advertising company. The advertiser loses out in such situations because it pays for advertising services that do not lead to sales, while the website owner benefits from the inflated billing revenues.

Judging by the amount of advertising for click-fraud services and software, click fraud is either common or often feared. We also know that savvy computer programmers can write java scripts to simulate user clicks, thereby automating click-fraud activities. Wikipedia notes that it is a felony in many jurisdictions—for example, is covered by Penal code 502 in California as well as the Computer Misuse Act 1990 in the United Kingdom. Several arrests have been made relating to click fraud.

Finally, it should be noted that a host's website personnel are not the only perpetrators of click fraud. Other possibilities include competitors seeking to deplete the advertising budgets of their targets, individuals seeking to damage the reputation of the host-publishers, misguided supporters of the host company (who seek to help it by increasing its ad revenues), and private vandals, who randomly target a particular company.

2-12. Spamming is the act of sending unsolicited emails to a large number of accounts—usually for advertising purposes. Spam is also a growing problem in instant-messaging, faxing, web-searching, and mobile-phone texting venues. One reason why spamming is of interest to accountants is because spamming is relatively costless to advertisers but relatively costly to recipients and Internet service providers who must transmit and deliver spam messages. In 2007, for example, the California legislature estimated that spamming costs the U.S. more than $13 billion in lost time and productivity. Spammers often attempt to pay ISPs for their data transmissions with stolen credit cards—an added cost.

Spammers require large lists of email accounts—the types of lists often found in accounting information systems. This makes AISs natural targets for spammers, and therefore a known security risk. The purpose or intent of spammers is also of concern to AISs, as a great deal of spam advertising is to sell pornography, perform an identity theft, or commit some other kind of fraud. Who has *not* gotten an unsolicited email from an African country, offering to share millions of dollars in exchange for the recipient's help in the U.S. and of course some additional small payments for "taxes" or other "transaction fees?" Finally, spammers clog the data transmission channels with their communications, adding to the total bandwidth required by the Internet.

Although students may argue that all spamming should be illegal, there are several counter arguments as well. Spammers can argue that some of their communications contain legitimate advertising, information that is of use to recipients, or valuable information about political activities or pending legislation. They might also claim that spam email is easily deleted, and often automatically filtered from recipient mail boxes. Wikipedia contains an extensive (and fascinating) discussion of spam at http://en.wikipedia.org/wiki/Spam_(electronic).

2-13. A *firewall* is an electronic barrier that limits access to corporate intranets or local area networks to bona fide users. Some firewalls are separate hardware systems while others are simply software programs installed on web servers. These firewalls are implemented by IT professionals. The specialized software in firewalls compares the IP addresses of outside users requesting information to current *access control lists.*

As noted in the text, firewalls are themselves limited in what they can do. For example, they cannot guard against certain forms of hacking such as *spoofing*—i.e., a hacker who uses a bonafide IP address to gain access to a system.

A *proxy server* is a computer and related software that acts as a gateway between internal corporate users and the Internet. One of the primary security functions of a proxy server is to control web access (e.g., to limit employee accesses to professionally-related sites). However, proxy servers can also run the software that creates internal firewalls.

2-14. *Data encryption* refers to transforming original, *plaintext* data into scrambled, *cyphertext* messages that cannot be understood even if it is intercepted during data transmission. The data used to encrypt (code) the message is called the *encryption key*.

Secret key encryption relies upon a shared algorithm and an encryption key that must be kept secret to be effective. *Public key encryption* uses two keys, a "private key" and a "public key," both of which must be known before a message can be decoded. These methods are discussed in greater detail in the text.

2-15. The three levels of authentication are (1) what you have, (2) what you know, and (3) who you are. An example of "what you have" is a driver's license with your picture on it. An example of "what you know" is a password. An example of "who you are" is a fingerprint or retina scan. Most business security systems depend on only one or two of these—rarely all three. High-level security in business and government environments might require all three.

Instructors are encouraged to ask students about different situations in which they had to use these different types of authentication. You might also ask students to recall movies such as *Mission Impossible* or *Entrapment*, where characters used advanced technologies to prove "who they are."

2-16. A *digital signature* is an electronic attachment that verifies and authenticates a business transaction (e.g., a purchase order, bidding document, or contract). The digital signature replaces a hand-written signature, which is difficult to transmit in non-graphic electronic documents. Like hand-written signatures, however, the objective of a digital signature is to assure the recipient that the document itself is legitimate and faithfully represents the intentions of an authentic sender. Thus, digital signatures are important on the Internet and value-added networks as a security tool.

2-17. Commerce is booming on the Internet, and most (but certainly not all) businesses have been able to boost both sales *and* profits as a result. Will all businesses do well? This is unlikely. However, the chapter notes that selling products and services on the Internet enables businesses to reach wider audiences, stay open around the clock, and maintain up-to-the-minute information on prices and products. Such selling also helps businesses reduce selling costs (because there is less sales labor and overhead-costs), inventory costs (because finished products are produced or ordered from suppliers in *response* to sales rather than in *anticipation* of sales), and processing costs (because sales and shipping documents are created by the buyer and/or the system). For businesses that sell many products, a web-based system requires a large investment in technology—both in upfront costs of development and ongoing costs of routine maintenance. Thus, most businesses must weigh the cost of building and maintaining a web presence against the additional revenues that such business generates. It is not a given that revenues will always offset costs.

The Internet provides opportunities as well as challenges for businesses. Thus, for individual companies, the Internet can spell "boom" or "bust," and students should be able to cite specific examples for both possibilities. To illustrate, the very smallest companies typically profit from a web presence because they are no longer limited to physical sales in local markets. At the same time, larger businesses feel increased pressure on prices and therefore profits due to the ease with which both retail and wholesale consumers now have access to a wealth of information and alternate sources for common goods and services.

This chapter provides several additional reasons why businesses can increase both sales *and* profits using Internet-based technologies. One example is the use of intranets and extranets to better secure LAN communications and increase access to and from trusted suppliers—possibilities that might decrease costs and therefore increase profits. Another example is the use of groupware to increase employee productivity. A third example is the expanded use of XBRL, which may enable a business to better report financial information and therefore reduce its accounting expenses (see Problems 2-20 and 2-21). Similar comments apply to firms that expand sales by accepting e-payments or reducing costs by expanding their e-business or EDI capabilities.

Problems

2-18. Acronyms:

a.	EC	electronic commerce
b.	EDI	electronic data interchange
c.	E-mail	electronic mail
d.	HTTP	hypertext markup language
e.	IDS	intrusion detection system
f.	IETF	internet engineering task force
g.	IP address	Internet Protocol address
h.	ISP	internet service provider
i.	URL	universal resource locator
j.	VANs	value-added networks
k.	VPN	virtual private network
l.	WWW	world wide web
m.	XBRL	extensible business reporting language
n.	XML	extensible markup language
o.	IDEA	interactive data and electronic applications
p.	SaaS	Software as a service
q.	ICANN	Internet Corporation for Assigned Names and Numbers
r.	DNS	domain name system (maintained by ICANN)

2-19. Depending on the sources of information used, the students may have a variety of different points about the advantages and disadvantages of implementing an intranet in the local company. Some of the main points that you would include in your "talking paper" are:

Disadvantages:

- Developing intranets requires an investment in time, money, and perhaps training
- Once created, an intranet must be maintained
- Intranets create a security hazard because shared information is potentially vulnerable to abuse
- Cloud computing companies may offer cheaper and better alternatives

Advantages:

- Intranets can be an important group collaboration tool
- Intranets allow companies to use existing web browsers
- Intranets can be a valuable method of sharing documents on a secure platform within the company
- The data stored on an intranet can be made secure so that proprietary data and information are only accessed by authorized users
- Intranets offer a wide variety of administration tools within the organization such as an online calendar (to schedule appointments, group meetings, and company-wide events), a task manager (for employees to keep track of their tasks, or those of their subordinates), a contact directory of employees, a list of e-mail accounts, and templates for corporate forms such as expense reports
- Intranets allow an organization to make databases available to authorized employees across the entire company
- Intranets can be scalable (i.e., can grow with the organization and/or its informational needs)
- Companies can frequently justify the cost of an intranet by quantifying some savings in operating costs (publish HR manuals, employee manuals, and other company publications on the intranet rather than paper copies)

2-20. This problem requires students to create their own HTML documents, using the example in Figure 2-1. It is important that students use Notepad or a similar word processor that stores data in ASCII (txt) format.

2-21. This problem requires students to log onto EDGAR and access the information from two companies. Note: the website has changed slightly. Students should click on the link "Company or fund name, ticker symbol, CIK (Central Index Key), file number, state, country, or SIC (Standard Industrial Classification)" instead of "Companies and other Filers." Instructors may get best use of this question if they require each student to obtain the financial information of a different company.

2-22. This problem requires students to log onto the XBRL home page and then (a) write a one-page summary of a new development and (b) select an article from those describing XBRL benefits and write a summary of it. For example, some of the benefits listed on the XBRL website at the time this instructor's manual was prepared include (1) improved business processes, (2) improved communications, and (3) enhanced business reporting through standardized tags.

2-23. This problem requires students to write a one page report on each of the items listed below. The answers to most of these questions may be found at: (1) www.xbrl.org, (2) http://accounting.smartpros.com (type XBRL in the search box to find many articles on XBRL), or (3) http://www.xbrleducation.com/.

a. History of XBRL. In April 1998, Charles Hoffman, a CPA in Tacoma, WA, investigated XML as a medium for the electronic reporting of financial information. He developed prototypes of financial statements and audit schedules using XML. Charlie contacted Wayne Harding, Chairman of the AICPA High Tech Task Force, in July 1998, about the potential of using XML in financial reporting. Charlie made a presentation to the AICPA Task Force in September of 1998. A more complete history of XBRL can be found at www.xbrl.org/history.aspx, and can be printed using the website www.xbrl.org/history-print.aspx. The AICPA was active in supporting the development of the language by funding a project to create prototype financial statements in XML.

b. XBRL Specifications. An explanation of XBRL specifications can be found by choosing "Specifications" from the main menu. "Specifications" provide the fundamental technical definition of how XBRL works. The current specification or version for XBRL is "2.1," but new ones may become available by the time you assign this problem in class. Current needs are for new formula, functions and taxonomy requirements.

c. Continuous Reporting. XBRL-tagged data enable businesses to create a steady stream of reports based on the underlying information, hence the term "continuous reporting." Three articles on this subject are: (1) Garbellotto, Gianluca (2009) "How to Make your Data Interactive *Strategic Finance* Vol. 90, No. 9 (March), pp. 56-57, (2) Chan, Slew H. and Sally Wright (2007) "Feasibility of More Frequent Reporting: A field Study Informed Survey of In-Company Accounting and IT Professionals" *Journal of Information Systems* Vol. 21, No. 2 (Fall, 2007), pp. 101-115, and (3) Robert Pinsker (2003) "XBRL Awareness in Auditing: A Sleeping Giant?" *Managerial Auditing Journal* Vol. 18, No. 9, pp. 732-736.

   Continuous reporting is an interesting concept. Generally speaking, the technology already exists for companies to report information more frequently than they currently do. Presumably, other reasons exist for not reporting more often (and certainly not daily or weekly!). One might be the familiar cost/benefit analysis, which suggests that companies do not believe the benefits of continuous reporting (or reporting more frequently than quarterly) outweigh their costs. A number of articles discuss the topic of continuous auditing. Some authors believe that continuous auditing is inevitable, while others suggest that this is not necessary. In any case, this question should start a lively dialog with the students regarding the future of IT auditing and the implications for corporate America. The following links provide several articles of interest:
   http://aaahq.org/AM2004/abstract.cfm?submissionID=1118
   http://accounting.smartpros.com/x43141.xml
   http://accounting.smartpros.com/x34375.xml

d. XBRL Required Reporting. The first conference on "Financial reporting in the 21st century: standards, technology, and tools" took place in Macerata, Italy, in September of 2011. The SEC now requires all public companies to file their financial

reports in XBRL format. Students who access the IDEA database will have no problem answering this question. The following websites identify industries and companies that currently produce financial statements in XBRL format:
http://www.edgar-online.com/xbrl/industry.asp
http://bryant2.bryant.edu/~xbrl

2-24. We ran out of Internet addresses because the number of different IP addresses available with 32 bits was insufficient to accommodate the global demand for different ones.

a. The value of 2^{32} = 4,294,967,296. Although this is a large number, the need for distinct addresses world-wide was even greater, and we ran out of them.

b. The new IP standard uses 128 bits. The value of 2^{128} is greater than 340,282,366,920,938,000,000,000,000,000,000,000,000 –a very large number that should satisfy our need for IP addresses for some time to come.

c. Several reasons probably account for why we have not run out of telephone numbers, despite their seemingly small size. These reasons include: (1) The base is "10" not "2" so the total number of combinations is 10^{10} = 10,000,000,000 or 10 billion. (2) These phone numbers are not free—each subscriber pays a monthly fee for them, whereas domain names (IP addresses) are virtually free. "Cost" serves to limit the demand for phone numbers. (3) Each country has a separate three-digit country code in addition to the 10 digits for the telephone number. This increases the number of phone numbers available worldwide by one thousand (= 10^3). Interestingly, cell phone carriers maintain their own systems, but use the same 10-digit addressing system. Additional carriers increase the *demand* for phone numbers, but the *supply* of phone numbers available for use.

2-25. This problem requires students to encrypt a message, using a simple cyclic substitution cipher. The encrypted message is:

BPWAM EPW QOVWZM PQABWZG IZM NWZKML BW ZMXMIB QB

2-26. This problem requires students to decrypt an encrypted message, using a simple cyclic substitution cipher. The decrypted message is:

Message 1: "It is not what we don't know that hurts us, it is what we do know that just ain't so."
Message 2: Justice delayed is justice denied.
Message 3: Too many cooks spoil the broth.

As suggested in the problem, this task becomes much easier if you use a spreadsheet. Here's an example for the last message:

Trial key:	12

Msg	Value	Value minus Displacement	Add 26 if required	New Letter
F	6	-6	20	T
A	1	-11	15	O
A	1	-11	15	O
Y	25	13	13	M
M	13	1	1	A
Z	26	14	14	N
K	11	-1	25	Y
Etc.	Etc.	Etc.	Etc.	Etc.

2-27. This problem asks students to write a one-page summary of an article they find online. Various accounting journals are going online. Besides the AICPA's *Journal of Accountancy* website, there is also the *ISACA Journal* (www.isaca.org), *Strategic Finance* (www.imanet.org) and *The CPA Journal* (www.cpajournal.com). An obvious advantage for readers is the ability to search the archives for articles on a specified topic online. The advantages to publishers include (1) making information more accessible to both members and non-members, (2) fulfilling organizational mandates to disseminate information, and (3) enabling users to search articles electronically for specific information or topics. To date, many journals do not charge for online access to articles, although some professional groups limit access to members. Instructors may wish to limit students to specific subjects or to articles less than one year old.

2-28. This problem involves the privacy statement of a fictitious company named Small Computers, Inc. As a general statement, online consumers have several concerns about computer security:

- They want to make sure that they will receive what they order
- They want their privacy protected
- They want a secure method of payment
- They want to be sure they will be billed only for what they purchased

Small Computers, Inc. addresses some of these concerns, but not all of them. For example, the company stresses privacy but does not say it will limit the use of its customer information to legitimate business purposes. The disclosure of business practices, shipping, and billing is reassuring. It will comfort the consumer to know goods are shipped at an early date and that the consumer need only accept items ordered. The return policy appears lenient although it does not state who is responsible for paying shipping on returned items. The statement about accidental billing actually may make a consumer aware that the chance for this exists.

Consumers are more likely to buy from a business online than they are off-line. They are also more likely to buy products with brand names. A business selling goods to end-

consumers online that does not have these characteristics will need to be extremely careful in crafting statements about privacy and business policies.

Case Analyses

2-29. This case requires students to select an accounting blog from the list provided in the question and write a one-page summary of their findings. Answers will vary by student.

2-30. Me, Inc. (The Do's, Don'ts, and Ethics of Social Networking Sites)

This case asks students to think about what to say, and what *not* to say, on social networking sites such as Facebook, Twitter, or LinkedIn. For example, Part 1 asks students to list four personal strengths. Some suggested answers to the various parts of this question are as follows:

1. Possible personal strengths: education, honesty, prior relevant work experience, willingness to learn, ability to commit to corporate goals, team player, good writing skills, and high IQ.

2. Possible red flags: prison or arrest record, making derogatory statements about the company, management, or immediate supervisor, membership in an extremist group such as a white-supremacy organization, overreactions to life reversals, reports of personal dishonest behavior, indications of overspending or excessive personal debt, evidence of drug use.

3. Some of the most popular networking sites are douban, Flixster, Friendster, Facebook, Habbo, LinkedIn, MyLife, MySpace, Netlog, Orkut (India), RenRen (China), Tagged, Twitter, and Vkontakte (Russia). Each of these has more than 50 million members. The website at http://en.wikipedia.org/wiki/List_of_social_networking_websites contains a list of over 200 social networking sites.

4. This part of the case asks students whether or not they would approve a high-level manager as a friend on Facebook. It is likely that students will be torn about this, not wanting to offend this manager but also not wanting him or her to read personal statements.

5. Is it ethical for a boss to fire an employee for postings on Facebook? Again, students are likely to not be sure about this. Are statements made outside of the work environment grounds for dismissal? Does it matter that such statements are written? Suggestion: after obtaining student feedback on this matter, ask them whether they would dismiss an employee under these same circumstances *if they were the boss*.

2-31. Anderson Manufacturing (Using XBRL-Enabled Software)

This case continues the systems studies of the cases in Chapter 8. At a minimum, instructors should require students to read Hammaker Manufacturing III to become familiar with the names of the individuals in this case.

1. XBRL-enabled software means that the software has the ability to create financial reports in XBRL format. It usually also means the ability to extract information *from* XBRL-formatted data. In this latter mode, you simply key in your request for information and quickly receive the data, the analysis, or graph(s) you desire. Finally, it means that software applications can import XBRL-coded data for analysis, further data processing, and archiving purposes. Today, most accounting packages provide XBRL formatting capabilities.

2. Figure 2-3 identifies a number of advantages that Lloyd might wish to discuss with Dick. The following articles are also available for additional benefits:

   http://www.cato.org/pubs/regulation/regv26n3/v26n3-13.pdf
   http://www.icaew.co.uk/library/index.cfm?AUB=TB2I_53335,MNXI_53335
   http://www.xbrl.org/faq.aspx

3. Each student's memo will be unique.

4. Several examples of XBRL PowerPoint presentations may be found on the Internet. Some examples can be found at:
   http://www.icgfm.org/XBRLPresentations.htm,
   http://www.xbrl.org/us/us/SanJose200601/Huh.pdf, and
   http://www.uhu.es/ijdar/documentos/Present04/Eric.pdf.

2-32. Barra Concrete (XOR Encryption)

This case requires students to use XOR operations to both encrypt and decrypt a message.

1. Applying the XOR cipher to the cipher message, we have:

Cyphertext:	0	1	0	0		1	0	1	1
Key:	1	1	1	0		1	1	1	0
XOR Result:	1	0	1	0		0	1	0	1

   This brings us back to the plaintext message of 1010 0101.

2: Applying the XOR cipher to each letter, we have the results shown below. The encrypted letters are shown in the XOR Result lines:

	Digit 1	Digit 2	Digit 3	Digit 4		Digit 5	Digit 6	Digit 7	Digit 8
G	0	1	0	0		0	1	1	1
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	0		0	1	0	0
O	0	1	0	0		1	1	1	1
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	0		1	1	0	0
,	0	0	1	0		1	1	0	0
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	1	1	0		1	1	1	1
T	0	1	0	1		0	1	0	0
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	1		0	1	1	1
E	0	1	0	0		0	1	0	1
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	0		0	1	1	0
A	0	1	0	0		0	0	0	1
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	0		0	0	1	0
M	0	1	0	0		1	1	0	1
Key:	1	1	0	0		0	0	1	1
XOR Result:	1	0	0	0		1	1	1	0