# I. Technology

1. Digital vs. Analog

a. List three devices or things that today are principally digital but were principally analog fifty years ago (that’s 1966):

<sound reproduction - phonographs>

<image reproduction - cameras>

<telephones>

<newspapers>

<television/video>

<movies/projectors>

b. Give **three reasons** behind these transitions from analog to digital

<error detection and correction, ability to deal with noise>

<compression, efficiency in transmission and storage>

<convenience in handling stored data>

<Moore’s law, availability of inexpensive digital processing, economics>

<possibly usability>

2. Suppose I want to mail several files, but the size of the collection of files totals more than my mail client will allow as an attachment. I run a utility (e.g. gzip) to compress) the files into an archive that is smaller than the mailer’s limit. The recipient of the message will be able to decompress (unzip) the archive to obtain the contents of the original file. archive.

The compressed files contain:

a. more b. less c. the same

information as the original files.

<the same>

Would an encrypted checksum of the compressed archive file be the same or different from an encrypted checksum for the original file? Explain your answer.

<different, because the change to the file will cause the checksum (encrypted or not) to differ>

3. We discussed the possibility of achieving “perfect secrecy” through encryption. Why is this approach to encryption rarely used in practice?

< it requires a key that is exactly as long as the data to be transmitted be shared between the sender and receiver. Could also mention that the key must consist of true random (vs pseudorandom) numbers>

4. The key bitwise operation performed in combining plaintext and keystream to generate ciphertext is called

<XOR>

5. Compare and contrast symmetric and asymmetric (public key) encryption methods with respect to the following

(a) relative speed

(b) number and types of keys used

(c) how it is customarily used (for example in setting up a secure communication channel)

<should mention at least:

speed: symmetric – fast; asymmetric -- slow

key mgmt.: asymmetric involves two keys, one of which is made public; symmetric only one key

domain of use: asymmetric used largely to exchange keys, symmetric to encipher large quantities of data>

6. We discussed different categories of attacks in Lecture 6. Suppose an attacker, in order to gain access to a system, bribes a developer to insert a backdoor into the login program. What is the general name for an attack of this sort?

<supply chain>

7. Now consider an attack in which the attacker notices that the microphone on a laptop can detect the sound of keys being pressed on the keyboard, and further, different keys make different sounds, so by turning on the microphone and monitoring the signal, the attacker can learn what the user has typed. What is the general name for this kind of attack?

<side channel>

# II. Policy

1. Which amendment to the U.S. Constitution protects U.S. citizens from unwarranted search and seizure, and what British colonial practice prompted its adoption?

<fourth amendment>

<Writs of Assistance, general warrants>

2. Compare and contrast the interests of law enforcement and foreign intelligence with respect to surveillance of electronic communications.

<should address law enforcement as targeted on prosecution and conviction vs foreign intelligence as dealing with foreign interests as opposed to law-breaking. Extra points if counter-terrorism is mentioned as adding complexity to the situation.>

3. What is the role of the U.S. judicial system when law enforcement requests electronic surveillance of a person or device?

<courts must decide whether or not to issue warrants for surveillance on the basis of whether probable cause has been demonstrated.>

4. The Foreign Intelligence Surveillance Court is different from other U.S. courts in that its proceedings are largely conducted in secret. In what sense is its role similar to that of other courts?

< It hears requests for surveillance activities in the sphere of foreign intelligenece and issues (or doesn’t issue) warrants permitting such surveillance.> <is this too hard?>

5. The TSA “No Fly” list is intended to prevent suspected terrorists from flying to or through U.S. airspace. In general, individuals cannot search the list, or see or alter their record (if they have a record) there. Which of the “Fair Information Principles” we discussed does this list NOT violate? (Give at least one)

<its existence is not secret>

<arguably, TSA takes reasonable precautions to insure the list is accurate and not misused>

# III. Critical thinking.

1. Do U.S. controls on the export of cryptographic devices influence the U.S. domestic market for encryption devices? Give an answer and explain your position.

<Either Yes or No is acceptable, as long as there is reasonable justification>

2. In *Report Of The Manhattan District Attorney’s Office On Smartphone Encryption And Public Safety*, November 2015. p. 18, it is proposed that a law be passed by Congress that The “would provide in substance that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked, or its data accessed, by the operating system designer. Compliance with such a statute would not require new technology or costly adjustments. It would require, simply, that designers and makers of operating systems not design or build them to be impregnable to lawful governmental searches.”

Provide an argument either in favor or against this proposal. Your choice of position will not affect your grade, but the logic of your arguments will.

Your position should address specifically:

a. Effects on technological innovation and global competitiveness of firms.

b. Effects on civil liberties and human rights.

c. Effects on technical requirements, including the effect of your position on the use of cryptography.

d. Effects on international relations.