Answer Key for Exam 1 in CPSC 457/557 (2013)

Answer 1:
a) Someone could buy the product for the developing-country price and "reimport" it for use in the US. He might, in fact, be able to buy the product in bulk in the developing country, reimport it, and sell it at a price that is significantly higher than the developing-country price but significantly lower than the US price. This could ruin the company's domestic market.
b) The language barrier prevents reimportation; few US consumers have use for the simplified-Chinese version of Windows.
c) Well known examples include "branded-pharma" prescription drugs and English-language textbooks. Full credit was given for any correct example.

Answer 2:
a) See Slide 23 of Lecture 2 (September 3, 2013).
b) False
c) False

Answer 3:
a) "Under the *secrecy paradigm*, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data [are] revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information." As computers and networks become more prevalent in daily life, less and less information is completely hidden; it makes less and less sense to say that no privacy interest is implicated when data that were revealed to one party for one purpose are collected or disseminated by another party for an entirely different purpose.
b) Information of all types, including personal information, has become increasingly accessible as computers and networks have become ubiquitous in everyday life. This increases the possibility of disclosure and of information's being exploited for purposes other than those for which it was originally collected. Many "public records," *e.g.*, court records, property deeds, and records of marriages and divorces, may in principle always have been accessible to the public, but they become *easily* accessible to everyone once they are put online; exploitation of such records that used to be costly becomes almost free.
c) *Identification*, which "can attach 'informational baggage' to people and inhibit their ability to change."

Answer 4:
a) The issuer is the signer of the certificate. The subject is the entity talked about in the certificate. See Slide 2 of Lecture 10 (October 1, 2013).
b) Impersonation of websites, mainly in the form of man-in-the-middle attacks. See Slides 22ff of Lecture 11 (Octber 3, 2013).
c) $\sigma_{RootCA_1,CA_2,PK_{CA_2}}$ and σ_{CA_2,Bob,PK_B}
d) $\sigma_{RootCA_2,CA_4,PK_{CA_4}}$, $\sigma_{CA_4,CA_3,PK_{CA_3}}$, and $\sigma_{CA_3,Alice,PK_A}$
e) $\sigma_{RootCA_2,CA_3,PK_{CA_3}}$ and $\sigma_{CA_3,Harry,PK_H}$

Answer 5:
A digital signature is a string of bits. If Alice produced the same bit string every time she signed a digital document, then someone other than Alice could copy that bit string onto other documents.

Answer 6:

a) False

b) False

c) True

d) False

e) True