EECE 412, Fall 2009

Quiz #2

Your Family name: _____

Your Given name: _____

Your student ID: _____

#	Points	Out of
1		4
2		12
3		17
TOTAL		33

Name of your left neighbor: _____

Name of your right neighbor: _____

Questions:

1. **Explain why a digital signature provides integrity protection:**

2. **Suppose R is a random challenge sent in the clear from Alice to Bob and K is a symmetric key known to both Alice and Bob. Which of the following are secure session keys and which are not? Explain your answer:**

   a) $R \oplus K$ is ___ secure, ___ not secure, because:

   b) E(R, K) is ___ secure, ___ not secure, because:

   c) E(K, R) is ___ secure, ___ not secure, because:

   d) h(K || R) is ___ secure, ___ not secure, because:

   e) $h(K \oplus R)$ is ___ secure, ___ not secure, because:

   f) h(R || K) is ___ secure, ___ not secure, because:

3. The handout contains a reproduction of new security-related features in MS Windows Vista.

a. **(7 points)** For each principle for designing secure systems, **put a checkmark** in the following table for those new features that **enable** or **follow** this principle.

Attention: The total number of points for this question will be determine using the following formula: $R - W$, where R is the number of right checkmarks and W is the number of wrong checkmarks.

	User Account Control	Bitlocker Drive Encryption	Windows Firewall	Windows Defender	Preventing exploits	Data Execution Prevention	Application isolation	Windows Service Hardening	Authentication and logon	Network Access Protection	x86-64 -specific features	Other features and changes
Least Privilege												
Fail-Safe Defaults												
Economy of Mechanism												
Complete Mediation												
Open Design												
Separation of Privilege												
Least Common Mechanism												
Psychological Acceptability												
Defense in depth												
Question assumptions												

b. **(10 points)** Write justification for the checkmarks in the above table.