SecureBoot (A)
1) How does the Xilinx secure boot process decide if a bitstream is encrypted?

Multiple choice:
1) Design security includes the following sub-catagories except
a) IC overbuilding
b) Trojan insertion
c) Bootstrap
d) Network firewalls

2) How does the Xilinx secure boot process decide if a bitstream is encrypted?
a) It starts to decrypt the bitstream and decides if it is gibberish
b) It looks for an encrypted-bitstream indicator in the bitstream
c) It consults the PS-side to determine if the user has indicated that an encrypted bitstream is provided
d) It consult the BBRAM and eFUSE embedded structures to see if they have been programmed

SecureBoot (B)
1) What is the first thing a Xilinx Zynq class FPGA does when it boots?

Multiple choice:
1) When a Xilinx Zynq class FPGA boots, it
a) First authenticates the FSBL and then decrypts it
b) First decrypts the FSBL and then authenticates it
c) Uses authenticated-encryption to both authenicate and decrypt the FSBL
d) Boots from the PL-side as usual

2) The best description of how the Self-Authenticated Secure Boot (SASB) process differs from the Xilinx secure boot process is given by
a) It loads the FSBL and then decrypts a 2nd stage boot loader U-Boot
b) It loads the FSBL and decrypts it before authenticating it
c) It loads the FSBL and then hands control over to FSBL to load the unencrypted SASB bit-stream
d) It loads the FSBL and then hands control over to the FSBL to load and decrypt the SASB bit-stream

SecureBoot (C)
1) Describes the two modes within SASB

2) Two segment style is used within SASB to allow

3) How is tamper detection within SASB accomplished?

Multiple choice:
1) The security properties of the SASB boot process include all of the following except
a) The SASB boot process is self-authenticating which can detect tamper
b) Any type of tamper with the HELP PUF helper data will prevent the system from booting
c) The key is transmitted off chip during enrollment in a secure environment
d) The helper data associated with the HELP PUF embedded within SASB does not leak information about the key

2) Tamper detection within SASB is accomplished by
a) By using a watch-dog monitor that scans the configuration data occassionally
b) By hashing the configuration data and comparing it with a secure digest
c) Zeroing out PL regions outside of SASB
d) Measuring path delays at high resolution

SecureBoot (D)
1) Where do the challenges for BulletProof come from?

Multiple choice:
1) SASB carries out dynamic partial reconfiguration using a blanking bitstream module to
a) Self-destruct when tamper is detected
b) Re-program unused portions of the PL with 2nd stage boot images
c) Destroy any hardware Trojans embedded into the unused portion of the PL
d) Zeros out portions of the SASB module when those modules have completed their function

2) A description of how BulletProof is different from SASB is best given as
a) BulletProof uses a functional unit as a source of Entropy and the FPGA configuration data is used as challenges
b) BulletProof times paths in the HELP modules as is true for SASB but uses configuration data as challenges
c) BulletProof uses a dedicated functional unit as a source of Entropy which has only one mode of operation
d) BulletProof boots from an encrypted bitstream and uses homomorphic encryption to generate the key