CPS 512 midterm exam #1, 10/5/17

Your name please: _____ NetID:_____ Sign for your honor:_____

Part 1. Digital Signatures (25 points). Suppose that a principal Alice (*A*) signs a message/record (*R*) that is received by another party Bob (*B*), who validates the signature. Suppose *R* is sent over an insecure network connection and that malicious Mark (*M*) can intercept *R* as it transits the network from *A* to *B*. Are the following statements True or False? Indicate your answer in the box at the **left** of each statement. You may comment further in the space on the right if you wish.

- (a) As *R*'s content grows in size, the size of its signature also grows.
- (b) As *R*'s content grows in size, the cost to sign or validate *R* also grows.
- (c) *M* must obtain B's public key in order to read (or decrypt) the content of *R*.
- (d) B must obtain A's public key in order to validate the signature of R.
- (e) *M* must obtain A's private key in order to modify the content of *R* without detection.

Part 2. Use Cases (40 points). Consider examples of such signed records *R* (as in Part 1) from systems we discussed.

(a) List four examples. Number them. Use names/keywords for the systems and records: don't explain how or why they generate or sign the records.

(b) For which of your numbered examples in (a) does the signed *R* contain the public key of *A* or *B* (or a hash of the key)?

(c) For which of your numbered examples in (a) does *R* contain the public key (or its hash) of another principal *C*, other than *A* or *B*?

(d) For each of the examples in (c), what other information does *R* contain about *C*?

Part 3. Blockchain (35 points). These questions apply to a blockchain system: a set of nodes organized in a broadcast network to maintain a global ledger of operations. You may presume that the blockchain functions like the example we discussed: Bitcoin. The ledger is broken into blocks; each node accepts the longest chain of valid blocks (that it knows of) as the current ledger.

(a) On average, how many nonces must a miner try before it finds a nonce that yields a block hash that begins with 4 leading zero bits?

(b) How many if the block hash must begin with 8 leading zero bits?

(c) Propose a strategy for the miner to select the candidate nonces to maximize its chances of finding a "good" one quickly.

(d) If the miner controls 10% of the computing (mining) power in the network, what are its chances of succeeding to "mine" the next block in the chain?

(e) How does a node in the network know the order of the blocks in the longest chain?

(f) How does a node in the network know the order of operations in the ledger?

(g) A malicious miner *M* could overwrite portions of the ledger history, if it can produce a new valid block chain that is longer than any other valid chain. What prevents this attack from succeeding?

Part 4. DNS (35 points). Google Public DNS (GPDNS) is a massive-scale DNS resolver that is open for use by any DNS client. Clients of GPDNS request lookups for complete domain names (e.g., *www.child.parent.net*), and the resolver returns DNS response records for the requested domain name.

(a) A lookup request for *parent.net* returns a DNS server IP address (call it *P*) that is authoritative for the domain *parent.net*. How does GPDNS determine the value of *P*?

(b) A lookup for *child.parent.net* returns "no such domain". How does GPDNS determine there is no such domain?

(c) Google says GPDNS responds faster (on average) than a local resolver, in part because GPDNS has many clients, including Google's search engines. How does more client activity help GPDNS serve its clients faster?

(d) GPDNS uses DNSSEC to validate lookups since 2013. How many decrypt operations does the resolver perform to validate that there is no domain *child.parent.net*?

(e) How does GPDNS obtain the public key for the DNS server (*P*) that is authoritative for *parent.net*?

(f) GPDNS uses a sharding scheme internally. It has the property that two lookup requests for the same domain name are likely to be handled by the same server. What is the benefit of this property?

(g) The GPDNS sharding has the property that two lookups for different domain names are likely to be handled by different servers. What is the benefit of this property?

Part 5. **Security of Google Public DNS** (60 points). Google contends that GPDNS is more secure than other DNS resolvers because their infrastructure is secure and implements best practices (including DNSSEC). Even so, Google suggests that clients communicate with GPDNS over a secure (SSL/TLS) connection to further protect DNS responses.

(a) For an SSL/TLS connection as explained in class (e.g., for HTTPS), how does the client obtain the session key to use with the connection? (10)

(b) How does the server obtain the session key to use with the secure connection? (10)

(c) How does this use of SSL/TLS to connect to GPDNS offer additional security for its users? To answer, summarize an attack that it prevents. (20)

(d) Is it secure yet? Summarize any other attack(s) that a client might be vulnerable to, relating specifically to its use of GPDNS. (20)

/25
/40
/35
/35
/60
/ 5
/200