Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets if necessary.

Total Marks: **30**

[10] 1. The article *Improving performance on the Internet* describes four approaches to content delivery:

(a) Centralized Hosting

(b) "Big Data Center"

(c) Highly Distributed

(d) Peer-to-peer

Describe briefly each of them; mention the "middle-mile."

Solution: Centralized Hosting consists in one, or very few, sites to host content. Commercial scale sites generally have at least two geographically dispersed mirror locations to provide additional performance. This is fine for small sites that cater to a localized audience.

"Big Data Center" architecture consists in caching and delivering customer content from a couple dozen high-capacity data centers connected to major backbones. This method, and the previous, are on the wrong side of the "middle-mile."

Highly distributed consists in a very highly distributed network, with servers in thousands of networks; by putting the servers within end-user ISPs, a highly distributed CDN is on the right side of the "middle-mile." Deploying this, however, is costly and time consuming.

P2P can be thought of as taking the previous scheme to its theoretical extreme, providing near infinity scalability. Unfortunately, the total download capacity of a P2P network is throttled by its total upload capacity.

[10] 2. Define the following terms:

(a) "Circuit-switched" versus "packet-switched" network communication

(b) "Pure ALOHA" versus "Slotted ALOHA" protocols

Solution: Circuit-switched networking depends on a dedicated connection or circuit between two points; a typical example is a traditional telephone system. Packet-switched, on the other hand, breaks a file into small chunks, that are routed independently to the destination, where they are re-assembled. Both Pure and Slotted ALOHA are "random access" & "common medium" methods of communication. However, in order to decrease the number of collisions, Slotted ALOHA implements a transmission window at fixed time intervals.

[10] 3. Suppose that $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ is a function with the following properties:

- for all $a, b, g \in \mathbb{N}$, $f(g, ab) = f(f(g, a), b) = f(f(g, b), a)$
- for any g, $h_g(c) = f(g, c)$ is a one-way function

Explain how f could be used for public key crypto in the style of Diffie-Hellman.

Solution: Suppose that we have a one-way function as in the question. First Alice and Bob agree on a public g and exchange it (the eavesdropper knows g therefore).

Then, let Alice generate a secret a and let Bob generate a secret b. Alice sends $f(g, a)$ to Bob and Bob sends $f(g, b)$ to Alice. Notice that because h_g is one-way, an eavesdropper cannot get a or b from $h_g(a) = f(g, a)$ and $h_g(b) = f(g, b)$.

Finally, Alice computes $f(f(g, b), a)$ and Bob computes $f(f(g, a), b)$, and by the properties of the function both are equal to $f(g, ab)$ which is their secret shared key. The eavesdropper cannot compute $f(g, ab)$ feasibly.