8 Concurrent and Distributed Systems (RNW)

(*a*) (*i*) Define the term *capability*. [2 marks]

(*ii*) What two fields must RBAC-based ACL entries always contain? [2 marks]

(*b*) Network-Attached Secure Disks (NASD) utilise *file managers* and *block servers*. File-manager RPCs exchange an authorised user ID, password, and object ID for a keyed cryptographic capability granting block access: $f(k, ObjID, rights)$.

(*i*) Describe the consequences of a user learning the value of key k. [2 marks]

(*ii*) Alice obtains a capability for object O_i. Bob then issues an RPC to the file manager revoking Alice's access to O_i. Describe what occurs when Alice performs her next block-server read on O_i. [2 marks]

(*iii*) Explain why it might be desirable, from a security perspective, to add a timeout field t, protected by the keyed hash, to the capability. [2 marks]

(*iv*) Developers extend NASD to support Quorum-replicated block servers. What new failure mode may arise during a Quorum block write, relative to unmodified NASD capabilities, in adding capability timeouts? [2 marks]

(*c*) The Andrew File System (AFS) is authenticated and encrypted using Kerberos; ACLs expressing positive and negative rights for users and groups. *Multiuser AFS clients* (e.g., UNIX servers) build a secure RPC connection for each local user, authenticated with their Kerberos ticket, and issue RPCs (e.g., file **read**) on their behalf only via their own connection. If no suitable Kerberos ticket is available (e.g., the ticket has expired, the user has destroyed their ticket, or a job is running unattended), then an insecure connection is used instead.

(*i*) The group *system:anyuser* holds the union of unauthenticated (anonymous) users and all authenticated users. Explain why an ACL granting read access to *system:anyuser* via a positive entry, but denying read access to user *rnw* via an overriding negative entry, might prove problematic. [2 marks]

(*ii*) Describe the consequences to AFS authentication and authorisation of a malicious local user gaining root access on a multiuser client. [2 marks]

(*iii*) An AFS client uses the unauthenticated Network Time Protocol (NTP) to synchronise its clock with the AFS server. Attacker Mallory is able to inspect, drop, and insert packets between the AFS client and server (e.g., by controlling a network switch). Describe an attack that allows Mallory to inject malicious content into the client's AFS cache, but that does not allow Mallory to write content directly to the AFS server. [4 marks]