Date ____ 20__

I.S Assignment 2
21K-3153

Q1a) If Alice's ticket does not contain a portion encrypted with Bob's secret key, then it is not genuine. Bob's secret key is known only to Bob and Kerberos Authentication Server. Bob decrypts ticket using his own secret key.

b) Bob can check authenticity of the ticket granting ticket in Alice's token. The ticket granting ticket (or TGT) contains Alice's identity & other info to generate a service ticket for Bob. Bob can also check the timestamp included in the token to check if it's not expired. When Alice is authenticated, her TGT is encrypted with Kerberos's key, shared with AS & TGS. When Bob receives token, if the TGT can be decrypted using his own secret key, token is genuine.

c) When Alice requests access from Bob, a ticket is generated by a Kerberos server which contains client's identity and session key. The session key allows for secure messages.

d) The ticket contains:
- Session key: generated by A.S, shared b/w Alice and Bob.
- Client Identity: This allows Bob to confirm that he is talking to Alice
- Timestamp & expiration time: ensures ticket is valid for a limited period.
- Service Information: Bob's identity
- Everything encrypted with Bob's secret key

Date ____ 20__

(a) Designed to address the problem of secure authentication in networks where multiple people have to communicate over unsecure networks.
Servers should be able to restrict access to unauthorised users and authenticate requests.

(b)
- User may alter network address of a workstation and send impersonated messages
- User may eavesdrop on exchanges & use a replay attack to gain entrance to a server
- User may impersonate another user from their workstation.

(c)
- Rely on each individual client workstation, to assure identity.
- Rely on each server to enforce a security policy based on user ID
- Require user to provide ID for each service
- Require systems to authenticate themselves to servers

(d) (i) Secure: eavesdroppers should not be able to gather info.
(ii) reliable: for all services that rely on kerberos for access control, lack of availability of kerberos means lack of those services
(iii) Scalable: Should support large number of clients & servers
(iv) Transparent: Beyond entering a password, user should not know authentication is happening.

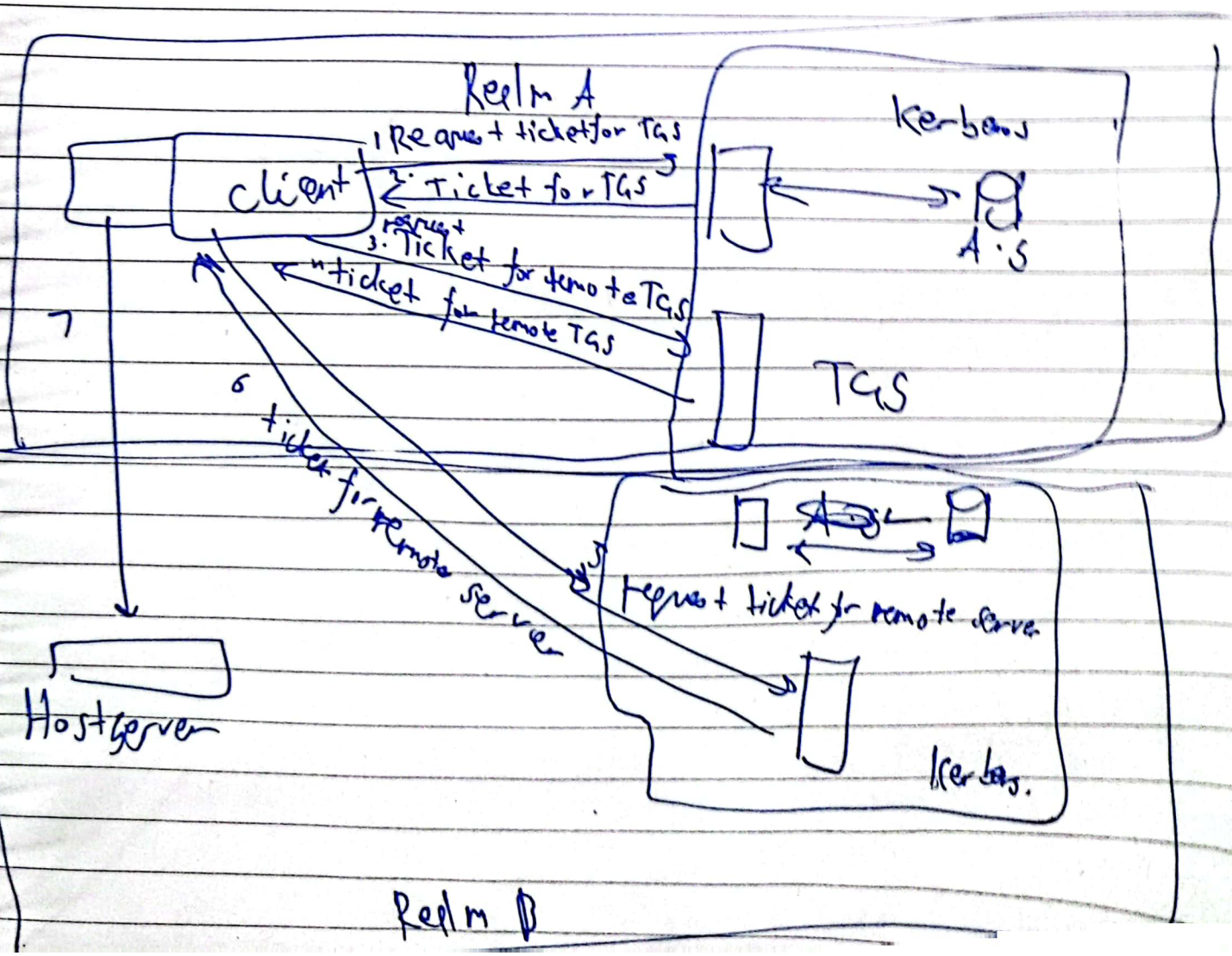
Date 20

(e) ~~A full service kerb~~

(e) (1) Server should have user IDs and passwords of all users registered

(2) A secret key should be shared with each server. All servers should be registered.

(f) Realms are logically grouped resources and Identities using kerberos. Managed by a key distribution center (KDC)



Date _____ 20___

Q3

(a) (i) $q = 157$ $a = 5$ ~~$X_A = 15$~~

$$Y_A = a^{X_A} \bmod q$$

$a = 5$ $q = 157$ $X_A = 15$

$$y_A = 5^{15} \bmod 157 = 79 \qquad Y_A = 79$$

(ii) $q = 157$ $a = 5$ $X_B = 27$ $Y_B =$

~~$Y_B = a^{X_B} \bmod$~~

$$Y_B = 5^{27} \bmod 157 = Y_B = 65$$

$Y_B = 5^{27} \bmod 57 = Y_B = 65$

(b) ~~p=3 q=7 e=5 n=10~~

(b) i p=3 q=37 e=5 n=10

n = 111

e=5 is co-prime to $\phi(n)=12$ and $<\phi(n)$

$de \bmod 12 = 1$ $d < 12$

$5 \times 5 = 25$ $25 \bmod 12 = 1$ so $d = 5$

PU = [5, 111] PR = [5, 111]

encryption: $10^5 \bmod 21 = 19$

decryption $19^5 \bmod 21 = 10$

Date _____ 20__

(iii) $p = 5 \quad q = 13 \quad e = 5 \quad m = 6$

$n = 65$

$\phi(n) = 48$

$e = 5$ & r. prime to 48 and < 48

$de \bmod 48 = 1 \qquad d < 48$

$145 \bmod 48 = 1 \qquad d = 29$

$25 \times 5 = 145$

$(48 \times 3 + 1) = 145$

PU = {5, 65} PR = {29, 65}

$E = \quad 6^5 \bmod 65 = 6$

$D = \quad 6^{29} \bmod 65 = 6$

(Q4) X.509 standard set the format of Public key certificates. The certificates are part of a public key infrastructure (PKI).

Chain of certificate refer to a sequence of certificate where each certificate is signed by the previous certificates issuer, forming a heirarchy. Starts with end-entity certificates and ends with root certificate.

Revokation is done is a certificate is no longer valid or compromised. done through a Certificate Revocation List (CRL) or online Certificate Status Protocol (OCSP)

b (a)

Certificate Issuance : issue a certificate
Certificate Revocation : revoke a certificate
Certificate Renewal : renew a certificate
Key management : generate, distribute & store keys
Certificate Validation : make sure certificate is issued by a trusted CA