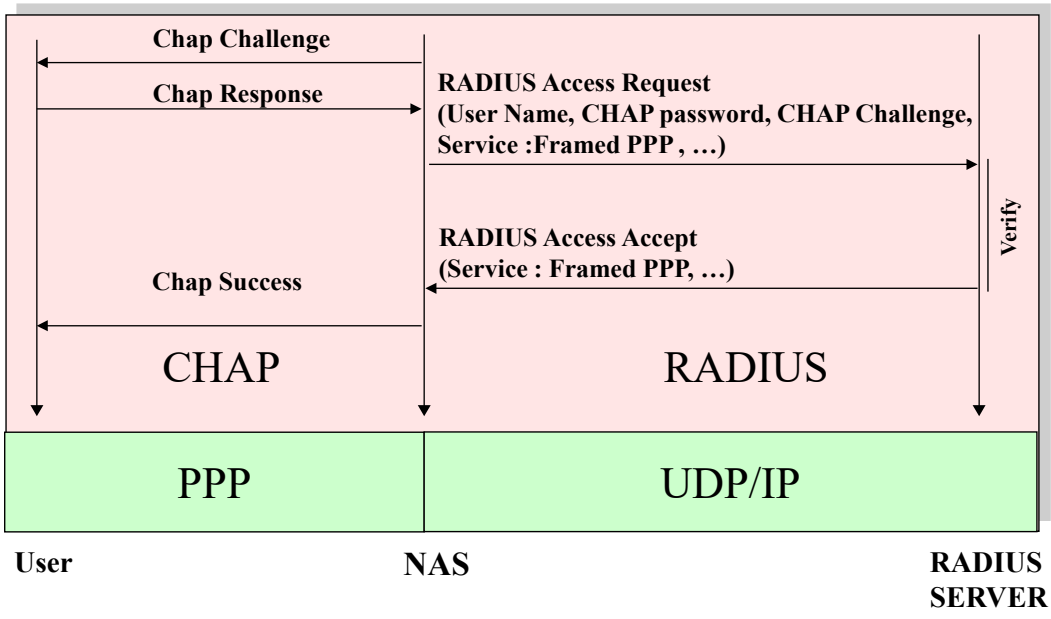
November 8, 2021, Midterm 1, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Briefly illustrate the main difference between a Relay and a Redirect agent in RADIUS

Q2: During the class we discussed vulnerabilities in the support of CHAP over RADIUS (see diagram on the right, taken from the slides of the class). Please i) briefly present what is the basic problem of (pre-1998) RADIUS that can be exploited here, and ii) show a concrete example of an attack.



Q3: You have to send a message M1 with integrity guarantees. Unfortunately, you know that an attacker has found a message M2 which collides with M1, i.e., H(M2)=H(M1). You cannot use HMAC, but you are forced to use as MAC either a secret suffix H(M,K) or a secret prefix H(K,M) construction. What would be your (least of evils) choice, and especially WHY?
[for simplicity in your considerations neglect patting and length fields in the hash]