Solution to HW #12, EE 578/CS 578, Fall 2000

(1)

Alice's public Key : $b_A = 2^3 = 8$

Bob's " " : $b_B = 2^5 = 32$

"Oscar's PK" : $b_O = 2^{16} = 156 \mod 467$

Alice comp. $K_{AO} = b_O^3 \equiv 173 \mod 467$

Oscar comp. $K_{AO} = b_A^{16} = 8^{16} \equiv 173$ "

Bob comp. $K_{BO} = b_O^5 = 156^5 \equiv 123$ "

Oscar comp. $K_{BO} = b_B^{16} = 32^{16} \equiv 123$ "

(2) a) Certificate will have Oscar's ID rather than Bob's
=> Alice will detect this directly

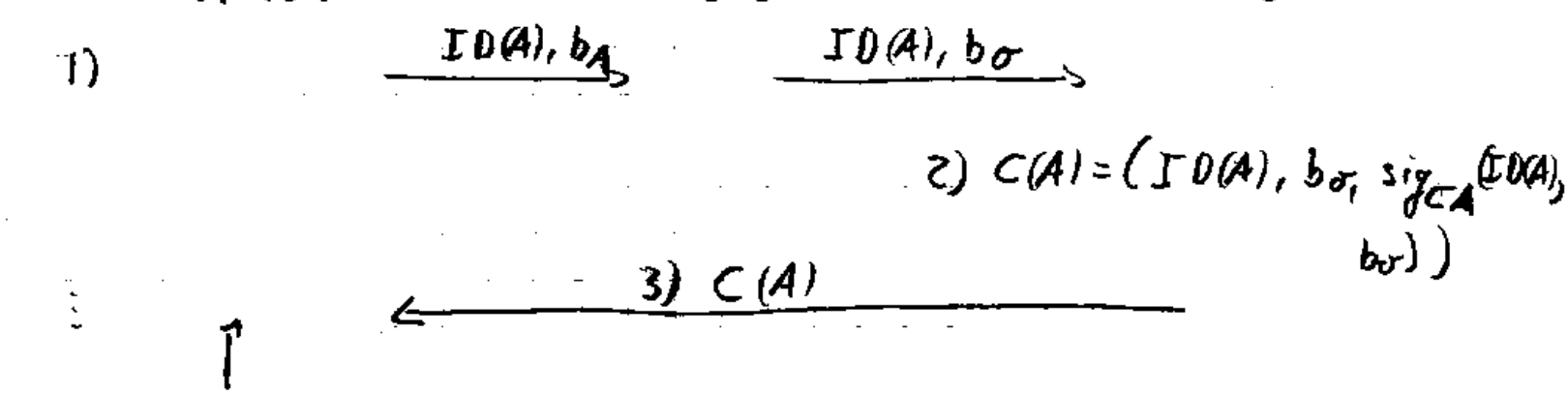
b) Certificate will not verify

(3)

Oscar		CA
$b_O = \alpha^{a_O} \bmod p$	$\xrightarrow{ID(A), b_O}$	$C(A) = (ID(A), b_O, sig_{CA}(ID(A), b_O))$ ← CA thinks it's Alice
	$\xleftarrow{C(A)}$	

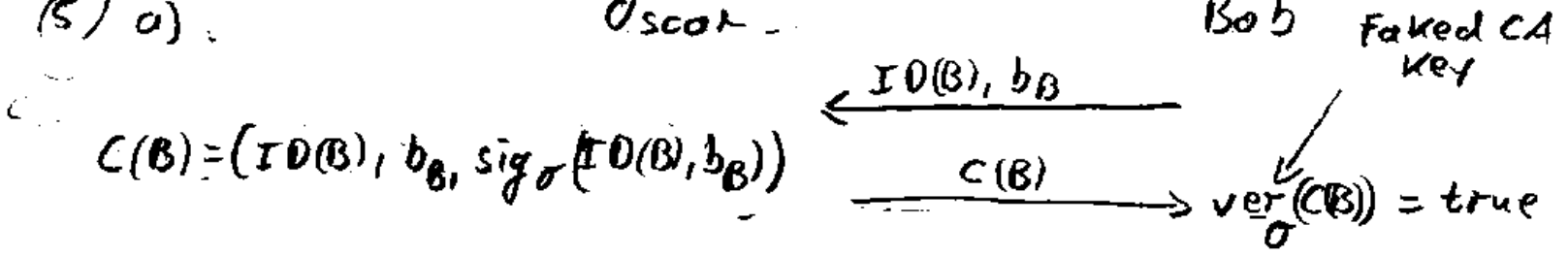
O-H: Oscar		Bob
$ver_{CA}(C(B)) = true$	$\xrightarrow{C(A)}$	
	$\xleftarrow{C(B)}$	$ver_{CA}(C(A)) = true$
$K_{BO} = b_B^{a_O} = \alpha^{a_B a_O} \bmod p$		$K_{BO} = b_O^{a_B} = \alpha^{a_B a_O} \bmod p$

④ certificate request:



Here it happens: Alice will compare her PK with the one in the certificate and see that it is forged. Note that Oscar can not manipulate the certificate itself in 3)

⑤ a)



b) Oscar Bob

generate faked certificate: $b_O = \alpha^{a_O}$