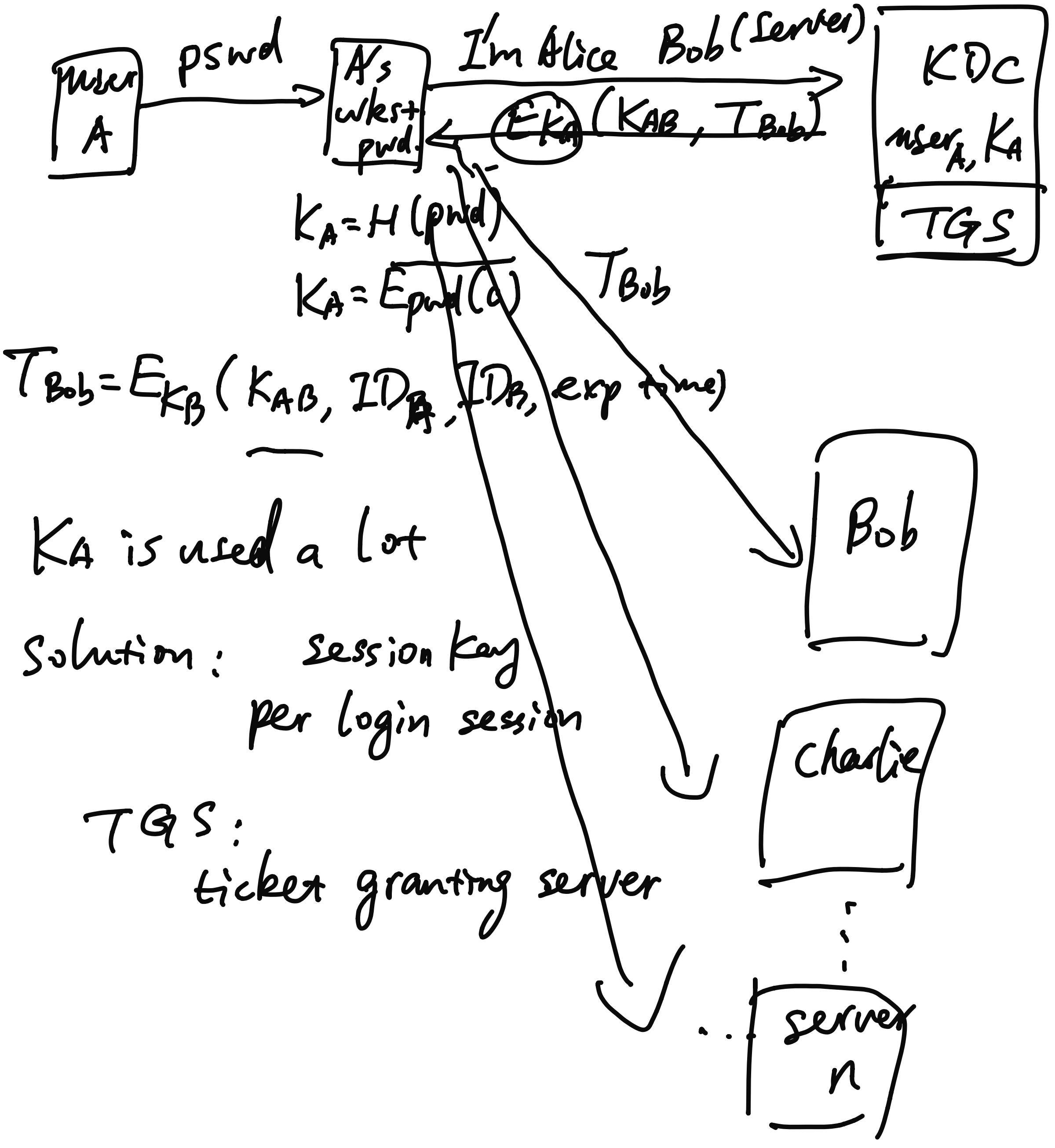
ECE 471/571. Kerberos (cont'd)



$K_A = H(pwd)$

$K_A = E_{\overline{pwd}}(c)$

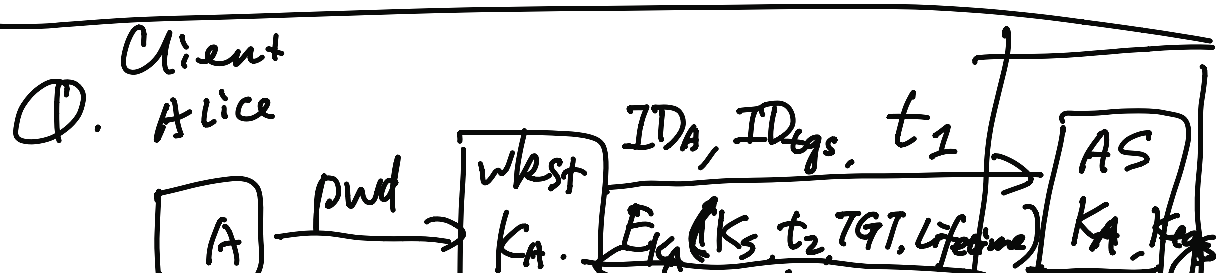
$T_{Bob} = E_{K_B}(\underline{K_{AB}}, ID_A, ID_B, \text{exp time})$

K_A is used a lot

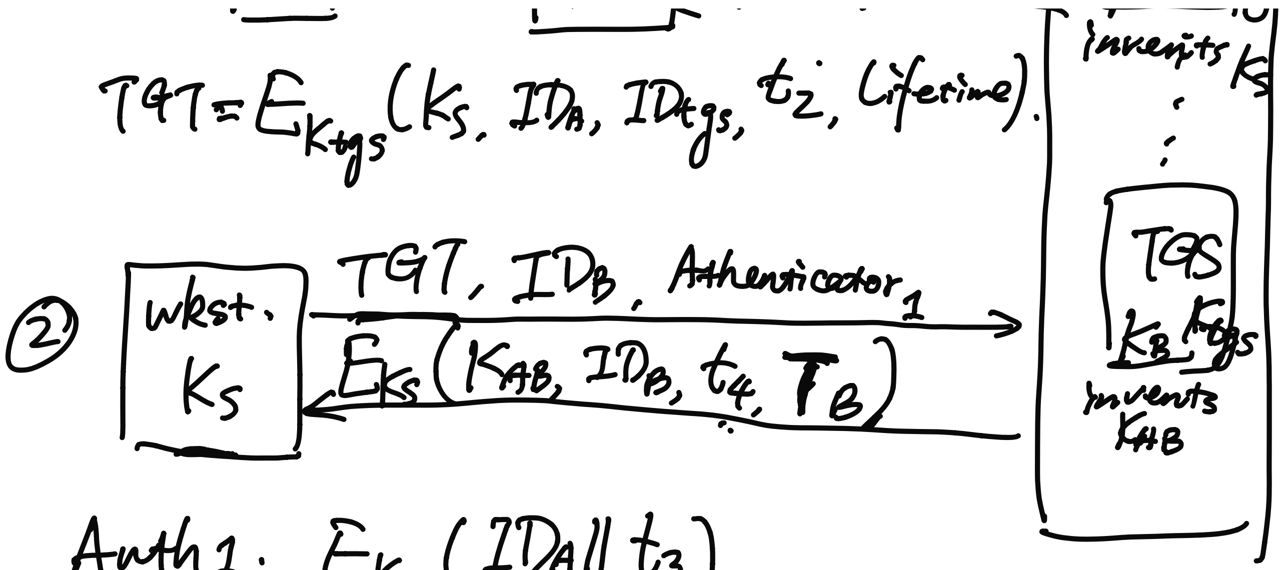
solution: session key per login session

TGS: ticket granting server

① Client Alice

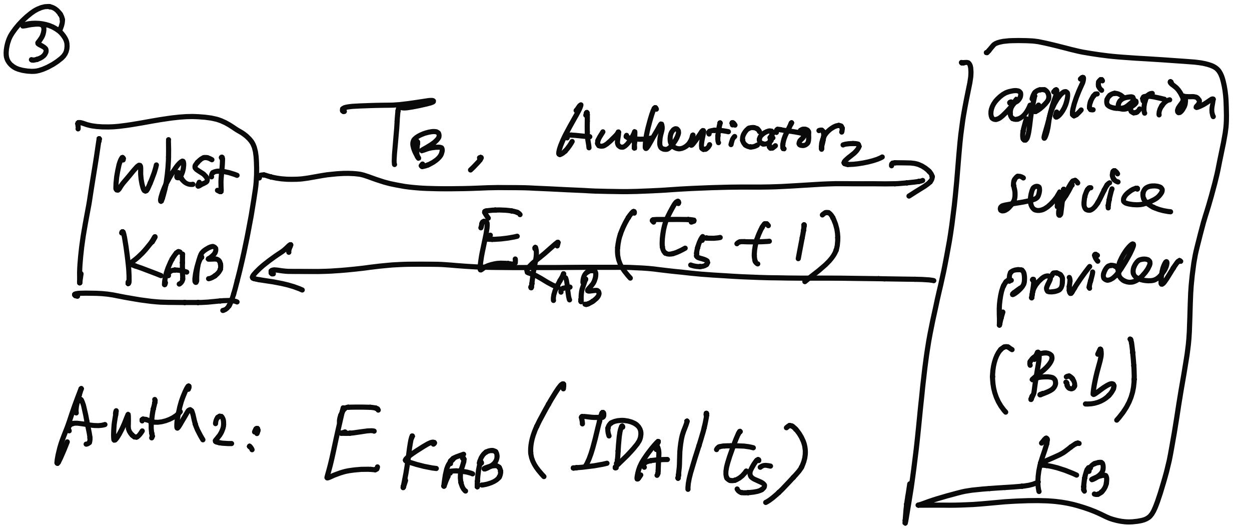


$TGT = E_{K_{tgs}}(K_S, ID_A, ID_{tgs}, t_2, \text{Lifetime})$.


invents K_S
②
wkst.
K_S
TGT, ID_B, Athenticator$_1$
$E_{K_S}(K_{AB}, ID_B, t_4, T_B)$
TGS
K_B, K_{tgs}
invents K_{AB}

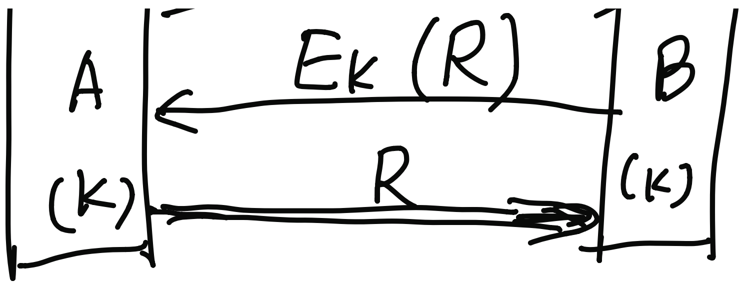
Auth 1: $E_{K_S}(ID_A \| t_3)$

$T_B = E_{K_B}(K_{AB}, ID_A \| t_4)$



Auth$_2$: $E_{K_{AB}}(ID_A \| t_5)$

types of nonce (# used once, fresh)



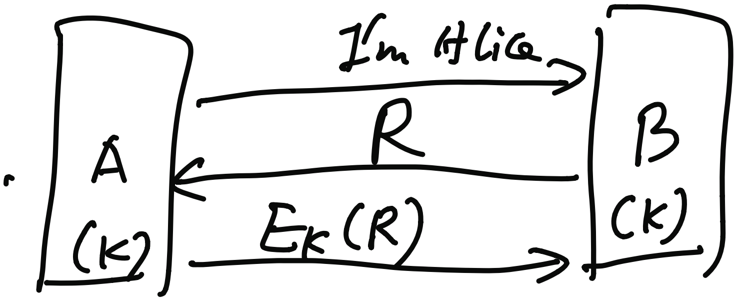
R is nonce

$R \in [1, 32]$ $\frac{1}{32}$

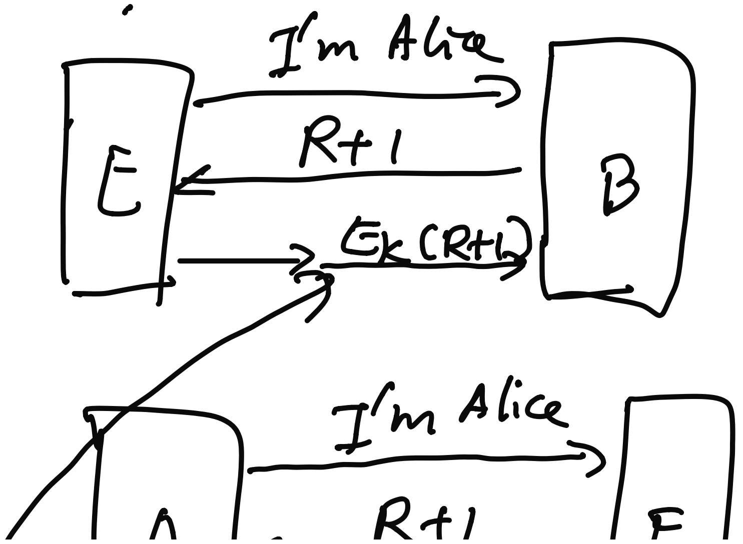
R must be random (unpredictable)

prob of guessing $\leq 1/2^{80}$

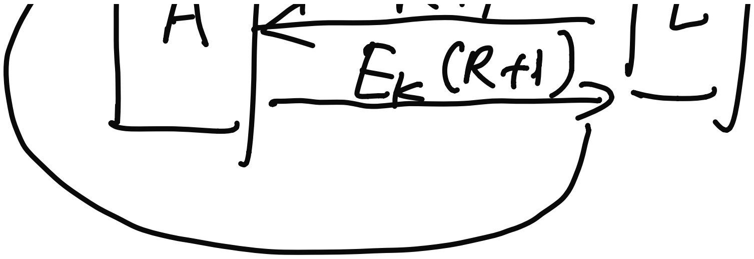
②.



Suppose R is counter / ts.

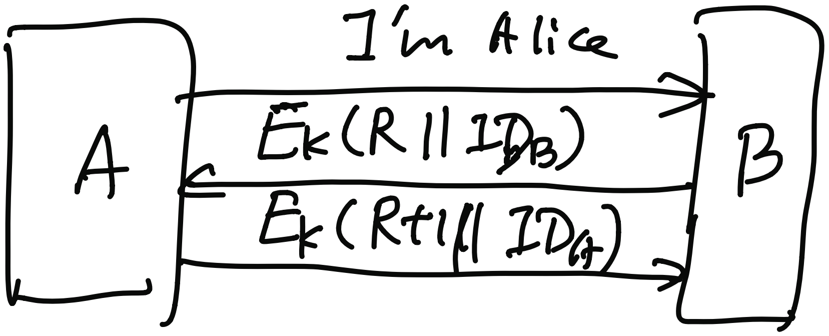


bucket brigade attack



R must be random

③



R can be predicatible
e.g t.s / counter