3. a) Originally, Sam would compute $B^a = g^{ab} \pmod p$ and Naum would compute $A^b = g^{ab} \pmod p$
However, after Malcolm's interception, Sam computes $C^a = g^{ac} \pmod p$ and Naum computes $C^b = g^{bc} \pmod p$

The values of the two integers b and c is what is hard to compute in efficient time, but since Malcolm already knows g^c,

$A = g^a$

$A^c = g^{ac} = g^{ca} = C^a$

$A^c = C^a$. Malcolm already knows A, c, and C

$a = c \log_C A$

Similarly, $b = c \log_C B$

Hence, calculating the secret keys becomes very easy.

b) Since Sam replaced both keys A and B with C, the encrypted message m' will be E(A, m) will be replaced with E(C, m) before the message reaches Naum and vice versa.

Decrypting m' is quite easy for Malcolm no matter who the sender is because he already know the secret key. Decrypting A or B with C will cause both of them to have an incorrect shared key.

c) The keys A and B were only shared once at the beginning, hence, Malcolm already intercepted it at that time and replaced it with C.
Therefore, although they will be able to succesfully communicate, the information sent and received will automatically be modified by the key C.