

Homework 2

Due: October 23, 2023

Points: 100

1. (10 points) In the Clark-Wilson model, must the TPs be executed serially, or can they be executed in parallel? If the former, why; if the latter, what constraints must be placed on their execution?
2. (20 points) An affine cipher has the form $c = (am + b) \bmod n$. Suppose m is an integer between 0 and 25, each integer representing a letter.
 - (a) Let $n = 26$, $a = 3$, and $b = 123$. What is the ciphertext corresponding to the phrase THIS IS A CIPHER MESSAGE.
 - (b) A requirement for a cipher is that every plaintext letter correspond to a different ciphertext letter. If a and b are not relatively prime to n , does the affine cipher meet this property? Either prove it does or present a counterexample.
3. (20 points) Alice and Bob are creating RSA public keys. They select different moduli n_{Alice} and n_{Bob} . Unknown to both, n_{Alice} and n_{Bob} have a common factor.
 - (a) How could Eve determine that n_{Alice} and n_{Bob} have a common factor without factoring those moduli?
 - (b) Having determined that factor, show how Eve can now obtain the private keys of both Alice and Bob.
4. (30 points) Needham and Schroeder suggest the following variant of their protocol:
 1. Alice \rightarrow Bob : Alice
 2. Bob \rightarrow Alice : $\{ \text{Alice}, \text{rand}_3 \}_{k_{\text{Bob}}}$
 3. Alice \rightarrow Cathy : $\{ \text{Alice}, \text{Bob}, \text{rand}_1, \{ \text{Alice}, \text{rand}_3 \}_{k_{\text{Bob}}} \}$
 4. Cathy \rightarrow Alice : $\{ \text{Alice}, \text{Bob}, \text{rand}_1, k_{\text{session}}, \{ \text{Alice}, \text{rand}_3, k_{\text{session}} \}_{k_{\text{Bob}}} \}_{k_{\text{Alice}}}$
 5. Alice \rightarrow Bob : $\{ \text{Alice}, \text{rand}_3, k_{\text{session}} \}_{k_{\text{Bob}}}$
 6. Bob \rightarrow Alice : $\{ \text{rand}_2 \}_{k_{\text{session}}}$
 7. Alice \rightarrow Bob : $\{ \text{rand}_2 - 1 \}_{k_{\text{session}}}$

Show that this protocol solves the problem of replay as a result of stolen session keys. *Hint:* Consider two cases: one in which the attacker does not send an initial message to Bob (that is, impersonate Alice in step 1), and the second where she does.
5. (20 points) Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not.