

CMSC 414: Hw 3 Solution

1. (text 9.2) Is this an example of an authentication scheme that ... guards against both eavesdropping and server database disclosure?

No. An attacker, say C, that sees the server database gets Z, the hash of Alice's password. Given Z, the attacker can impersonate Alice:

C (has Z)	B (Bob) (has Z)
<ul style="list-style-type: none"> send [A, B, conn] to B send [hash(Z, R)] to B 	<ul style="list-style-type: none"> send challenge R to A received msg matches hash(Z,R) so B assumes sender is A

2. (text 9.3) Extend the scenario in §9.7.4.1 to a chain of three KDCs, say X, Y, and Z, where A wants to talk to B, X is A's KDC, Y is B's KDC, and Z is a KDC that has shared keys with X and Y.

A (has K_{AX})	X (has K_{AX}, K_{XZ})	Z (has K_{XZ}, K_{ZY})	Y (has K_{ZY}, K_{YB})	B (has K_{BY})
<ul style="list-style-type: none"> send [A wants to talk to Z] to X send [A wants to talk to Y] to Z send [A wants to talk to B] to Y 	<ul style="list-style-type: none"> generate session key K_{AZ} send [K_{XZ}{talk to A; use K_{AZ}}] to Z send [K_{AX}{talk to Z; use K_{AZ}}] to A 	<ul style="list-style-type: none"> generate session key K_{AY} send [K_{ZY}{talk to A; use K_{AZ}}] to A send [K_{AZ}{talk to Y; use K_{AZ}}] to A 	<ul style="list-style-type: none"> generate session key K_{AB} send [K_{BY}{talk to A; use K_{AB}}] to B send [K_{AY}{talk to B; use K_{AB}}] to A 	