Instructor Notes for the "Key Types" Scenario
May 15, 2007

The key type scenario illustrates some potential cost of ownership differences between symmetric and public key cryptography. The scenario uses relatively low motive assets, and cryptography that is embedded as part of an application.

The scenario begins with two users within an office who need to exchange secret messages using a hypothetical "messaging" program. These users have locked offices, but must use a LAN that is subject to sniffing by other employees.

Initially, the users employ message software that has no encryption. The player must purchase similar software that performs encryption. Otherwise, a nosy employee sees their secrets. The scenario does not address differences between application-based encryption and other techniques such as VPN's or SSL.

Players have a choice between a messaging software product that uses symmetric key encryption and one that uses public key encryption for key management. The latter has a higher setup cost, but a smaller incremental cost as new users are added.

After the player selects an encrypting messaging product, a third user is added. The player must provide this third user with messaging software that is compatible with that used by the other two users. If the player sticks with symmetric key encryption, there is a lot of cost and complaint.

Players are then confronted with users who are cracking other user's passwords. Plain text hashes of passwords are transmitted via the network from workstations to a central server. Players cannot change that. The player must set a password policy on the server to prevent users from selecting weak passwords.