

Re: Key exchange

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00543.html>

- *From:* Anne & Lynn Wheeler <lynn@xxxxxxxxxx>
 - *Date:* Sun, 16 Jul 2006 10:00:20 -0600
-

"John E. Hadstate" <jh113355@xxxxxxxxxx> writes:

This pretty well describes how most cryptographic hashes are used to create keys. See your email for PDFs and diagrams on how to use hash functions to generate cipher keys from passwords.

there is similar stuff for "derived" keys ... i.e. financial industry derived unique key per transaction ... search on DUKPT ... for instance see reference to DUKPT & X9.24 in this old nist document:
<http://csrc.nist.gov/CryptoToolkit/aes/pre-round1/comments.pdf>

also transit systems with magstripe or "memory" chips ... and various other infrastructures have derived keys. there is system-wide master key (for transit systems in each processor connected to turnstiles). the card is read containing account number and encrypted information. the combination of of the system master key and account number is used to calculate the card-specific derived key, the information is decrypted, updated, re-encrypted, and then written back to the card (systemic risk countermeasure to brute force attack on a single system-wide symmetric master key)