Algorithm Areas

Tim Hudson – Cryptsoft
tjh@cryptsoft.com
Secret Management

• Threshold / Split Key Schemes
• Mnemonic Codes
• Group Schemes
Threshold / Split Key Schemes

• Shamir’s Secret Sharing
  • Interoperability
    • Selection of Polynomial
    • Selection of Generator for Polynomial
    • Test Vectors
  • Practical Issues
    • Format of Splits

• Long term recovery of secrets requires a standard mechanism and broad support

• Ref: McGrew TSS, RSA BSAFE, Bitcoin Shamir Secret Sharing
Mnemonic Codes

• Human Data Entry
  • Entry of raw material of reasonable length is subject to error
  • Checksums can help catch errors – but don’t ease entry
  • Mnemonic Codes sorts this out
  • Allows for clearer communication via voice (phone)
  • Requires a standard word list
    • Careful selection of words
    • Avoid similar words

• Ref: NATO phonetic alphabet, PGP Word List, Bitcoin Key Recovery Codes
Group Schemes

• **Group Schemes**
  • In threshold schemes some parties are more trusted than others
    • E.g. two C-level or one C-level and two directors etc
  • Effectively a split of splits

• **Interoperability**
  • Expression of group requirements
    • Need to be able to inform the user as to what groups require which thresholds
  • Test vectors
  • Performance
  • Ease of implementation

• **Ref:** AES GF($2^8$)
General

• Human error
  • Need checksum for confirmation
  • Need ability to indicate what is required for input
Summary

• Common Problem
• No widespread defined standard
• Many approaches used
• Interoperability challenges