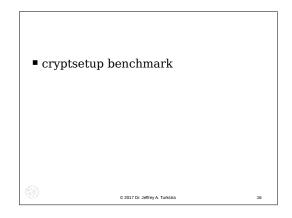
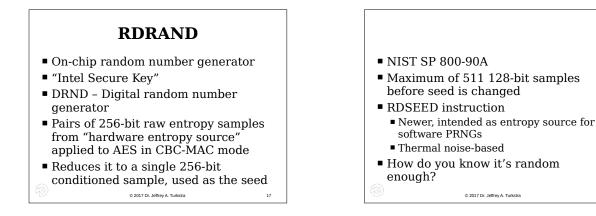


AES instruction set

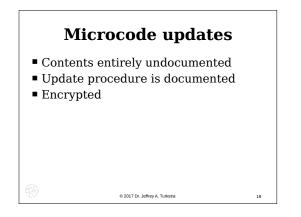
- ASENC: One round
- AESNCLAST: Last round
- AESDEC: One round decryption
- AESDECLAST: Last round decryption
- AESKEYGENASSIST: Assist in AES round key generation
- AESIMC: AES Inverse Mix Columns
- PCLMULQDQ: Carryless multiply

© 2017 Dr. Jeffrey A. Turkstra





15



Executing where we shouldn't Since 80286, preventable with segmentation Most OSes: we want it flat

© 2017 Dr. Jeffrey A. Turkstra

20

