Cloud Security: Alice and Bob Go to Washington

Jon Callas, Tamzen Cannoy, Nicko van Someren

Cloud Security: Alice and Bob Go to ~~Washington~~

Jon Callas, Tamzen Cannoy, Nicko van Someren

Cloud Security: Alice and Bob Go to *Heaven*

Jon Callas, Tamzen Cannoy, Nicko van Someren

Alice

- Is a good lady
- Works with children
- No question of getting her in

Cloud Security Services

- Alice uses Decomposable Credential to authenticate with St. Peter
  - After death, composable credentials not appropriate
- Sends DC to SaaS (Seraphim-as-a-Service)
- Alice gets Cryptographic Key to Heaven

Protocol Complete

Bob

- Not of the right religion
- Bob wants St Peter to cut him some slack…

Cryptographic Access to Heaven

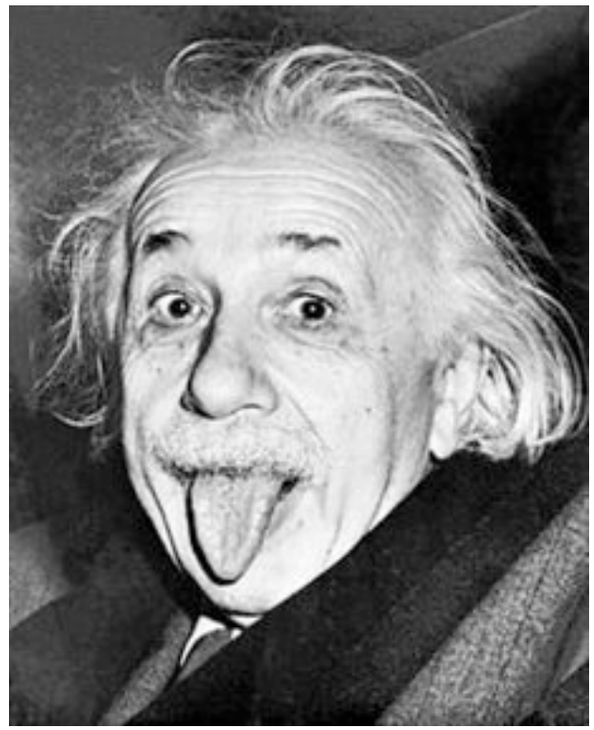
- St Peter holds Keys to Heaven
  - Protected with Angelic Encryption Standard (AES) since 2002
- Bob needs to cryptanalize AES

Description of AES

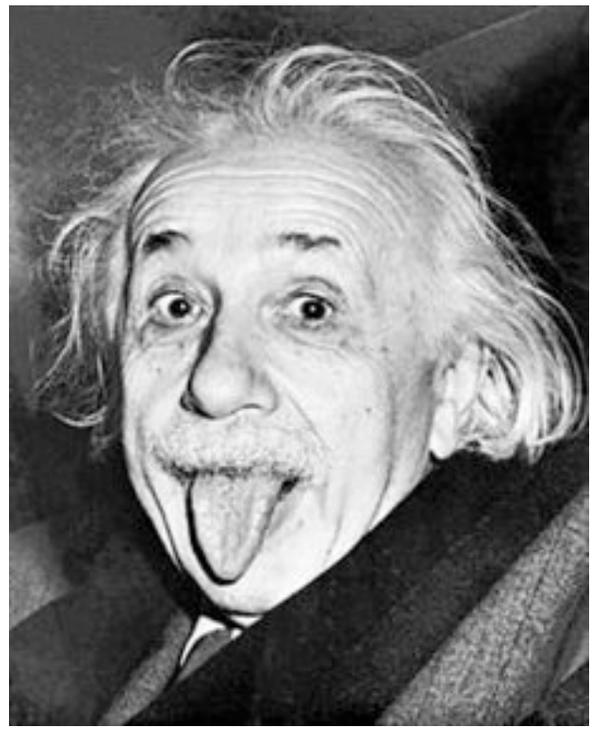
- Quantum crypto rejected

Description of AES

- Quantum crypto rejected
  - God does not play dice

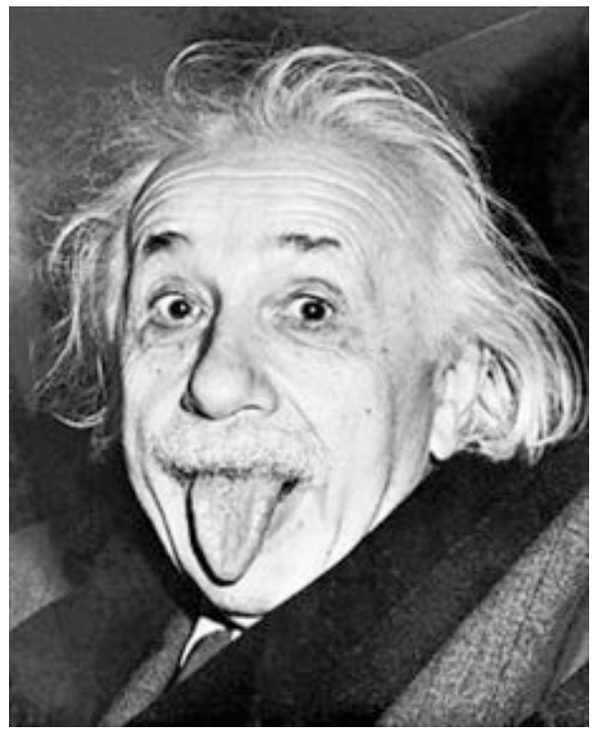


Description of AES



- Quantum crypto rejected
  - God does not play dice
- God does play cards, though
  - AES uses fully unbalanced Thorpe Shuffle

Description of AES



- Quantum crypto rejected
  - God does not play dice
- God does play cards, though
  - AES uses fully unbalanced Thorpe Shuffle
- Number rounds specified to be the number of angels dancing on the head of a pin
  - Allows for fully parallel implementation

Cryptanalysis of AES

- Omniscient Oracle Model
  - All rounds known, just not public
    - Since all rounds known, reduced round attacks are actually practical
- Recent cryptanalysis also shows it is completely vulnerable to related key attacks

Problems of Omniscience

- The Omniscient Oracle also knows that AES is vulnerable to related key attacks
  - Won't answer questions about related keys
- Bob needs a new strategy

Unrelated Key Attack

- Bob queries the Omniscient Oracle for relationships about all bits in key K
  - Uses divertable and subliminal zero-knowledge proofs to find where there is no relation

The Sublime Diversion

- For each bit in hypothetical K', Bob queries the Omniscient Oracle for relationships between K[i] and K'[i]
  - Bob constructs completely unrelated key K' where all bits are unrelated to bits in K
  - Invert K' to get K
  - Solution in O(*N*) time, irrespective of number of rounds

Attack Complete

Postscript

- Bob finds a suitable co-author
- Bob writes up details of the attack
- Bob publishes results
  - (How do you think we got them)
- Bob gets Erdös number of 1