Why Random Numbers for Cryptography?

Miles Smid

Orion Security Solutions

Short Answer:

Because we need to improve the overall quality of our RBGs and how we implement them.

Historical: Key and IV Generation

- “A DES key consists of 64 binary digits (“0”s or “1”s) of which 56 bits are randomly generated and used directly by the algorithm.” (FIPS 46, 1977)
- DES Modes of Operation (FIPS 81, 1980) uses IVs as “randomizing” blocks for CBC, CFB, and OFB modes
- Financial Institution Message Authentication (ANSI X9.9-1982) makes use of keyed DEA
- Message or Data Authentication Codes using DES (FIPS 113, 1985) points to ANSI X9.17 for key generation of keys
- Idea: Use block cipher to generate pseudo-random blocks

Historical: RNG for Financial Institution Key Management (ANSI X9.17-1985)

K* = (K1,K2) = secret key pair

$TDEA_{K*}(X)$ = TDES encryption of X

S = secret seed

1. DT = date time
2. I = $TDEA_{K*}(DT)$
3. R = $TDEA_{K*}$(I XOR S) = Deterministic Random Output
4. S = $TDEA_{K*}$(R XOR I)
5. Go to step 1.

Asymmetric Key Generation

- The Digital Signature Standard (FIPS 186) provides several DRNGs to generate pseudorandom values
  - Private key x such that $0<x<q$ where q is a prime divisor of $p-1$.
  - Secret internal value k such that $0<k<q$
- Idea: Can use a hash function to generate pseudorandom values
- These RNGs were intended for generating integers modulo q rather than blocks
- These functions are used as general non-deterministic RNGs
- Little or no advice about seed generation was provided

Other Uses

- PIN and Password Generation
  - PIN Protection Principles, ANSI X9.8:1
  - Password Generation, FIPS 181-1993
- Generation of Primes
  - DSA, ANSI X9.30
  - RSA, ANSI X9.31
  - Prime Number Generation, ANSI X9.80
- Random Challenges for Authentication
  - Entity Authentication using PKC, FIPS 196
- Key Confirmation
  - ECC Key Agreement and Transport, ANSI X9.63
  - NIST Key Schemes Recommendation
- Nonces

FIPS 140-1&2 RNG Requirements

- Use of an approved RNG for key generation
- Continuous RNG Test
- Statistical Tests
  - Laboratory validation tests
  - Self tests
- Idea: “Compromising the RNG shall require at least as many operations as determining the value of the generated key.”

Why ANSI X9.82?

- Need for general guidance on RBGs for cryptographic applications
- Need for application independent RBGs
- Need for guidance on seed generation
- Need for best guidance on development of non-deterministic RBGs
- Need for more comprehensive validation tests (without going overboard)
- Need for in depth consideration that is provided by standards development
- Need to improve overall quality of cryptographic RBGs

Related Efforts

- U.S. Government development and use of X9.82 techniques and methods

- ANSI X9.82 Concepts submitted as input to ISO/IEC CD 18031. (See Debby Wallner)

And Now,
DANSI X9.82