Random Number Generation Workshop  
July 19-22, 2004  
National Institute of Standards and Technology (NIST)

Monday, July 19th: Lecture Room A, Building 101  
Topic focus: Part 1, Overview and Basic Principles  
9:00 - 9:15  Welcome (Elaine Barker)  
9:15 - 9:45  History of the Project (Miles Smid)  
9:45 - 10:15  Strategy (Paul Timmel)  
10:15 - 10:30  Break  
10:30 - 11:30  Part 1 Presentation (Don Johnson)  
11:30 - 12:30  Lunch  
12:30 - 1:30  Part 1 Presentation (continued)  
1:30 - 1:40  Break  
1:40 - 2:30  Part 1 Presentation (continued)  
2:30 - 2:45  Break  
2:45 - 3:45  Part 1 Discussion of Issues (Moderator: Paul Timmel)  
3:45 - 4:00  Break  
4:00 - 5:00  Discussion of Part 1 Issues (continued)

Tuesday, July 20th: Lecture Room A, Building 101  
Topic Focus: Part 3, Deterministic Random Bit Generators (DRBGs)  
9:00 - 10:15  General Presentation of Part 3 (Elaine Barker)  
10:15 - 10:30  Break  
10:30 - 12:00  Hash-based and Block-cipher-based DRBGs (John Kelsey)  
12:00 - 1:00  Lunch  
1:00 - 1:30  Number Theoretic DRBGs (Don Johnson)  
1:30 - 2:30  Operational and Validation Testing (Moderator: Elaine Barker)  
2:30 - 2:45  Break  
2:45 - 3:45  Discussion of DRBG Issues (Moderators: Elaine Barker and John Kelsey)  
3:45 - 4:00  Break  
4:00 - 5:00  Discussion of DRBG Issues (continued)

Wednesday, July 21st: Lecture Room A, Building 101  
Topic Focus: Part 2, Non-Deterministic Random Bit Generators (NRBGs)  
9:00 - 9:15  Review of NRBG terms (Mike Boyle and John Kelsey)  
9:15 - 10:15  Strategy and NRBG types (Mike Boyle)  
10:15 - 10:30  Break  
10:30 - 11:30  Entropy Sources (John Kelsey)  
11:30 - 12:30  Lunch  
12:30 - 2:30  Discussion of NRBG Issues (Moderators: Mike Boyle and John Kelsey)  
2:30 - 3:45  Discussion of NRBG Issues (continued)  
3:45 - 4:00  Break  
4:00 - 5:00  Discussion of NRBG Issues (continued)
Thursday, July 22\textsuperscript{nd}, Lecture Room A, Building 101

Topic Focus: Miscellaneous

9:00 - 10:00  Testing Issues with Operating System-Based Entropy Sources (Peter Gutmann)
10:00 - 10:15 Validation and NIST Statistical Test Status (Larry Bassham)
10:15 - 10:30 Break
10:30 - 11:30 Parking Lot Discussions (Moderator: Debby Wallner)
11:30 - 1:00 Lunch
12:30 - 2:30 Parking Lot Discussions (continued)
2:30 - 2:45 Break
2:45 - 3:45 Holistic Discussions (Moderator: Debby Wallner)
3:45 - 4:00 Break
4:00 - 4:45 Holistic Discussions (continued)
4:45 - 5:00 Wrap up (Elaine Barker)