The Second
Advanced Encryption Standard (AES)
Candidate Conference

March 22-23, 1999

Hotel Quirinale
Rome, Italy

****

AGENDA

****

Day 1 – Monday, March 22

8:00 – 9:00

- ❑ Registration, material distribution
- ❑ Coffee

9:00 **Introduction -** Welcome and Overview (*William Wolfowicz and Miles Smid)*

9:30 **Session 1: Surveys (I)** – *Tom Berson (chair)*

- ❑ NIST's Round 1 Efficiency Testing *(NIST)*
- ❑ "Implementation Experience with AES Candidate Algorithms" *(Brian Gladman)*
- ❑ "Performance Comparison of the AES Submissions" *(Bruce Schneier)*
- ❑ "AES Java™ Technology Comparisons" *(Alan Folmsbee)*

11:00 Break

11:30 **Session 2: Surveys (II)** – *Anatoly Lebedev (chair)*

- ❑ "Report on the AES Candidates" *(Serge Vaudenay)*
- ❑ "Instruction-level Parallelism in AES Candidates" *(Craig Clapp)*
- ❑ "A Note on Comparing the AES Candidates" *(Eli Biham)*
- ❑ NIST's Round 1 Randomness Testing *(NIST)*

13:00 Lunch (provided)

14:30 **Session 3: Smart Cards (I) – Implementations** – *Craig Clapp (chair)*

- ❑ "cAESar results: Implementation of Four AES Candidates on Two Smart Cards" *(François Koeune)*
- ❑ "Performance Analysis of AES candidates on the 6805 CPU core" *(Geoffrey Keating)*

15:30 Break

16:00-17:15 **Session 4: Smart Cards (II) – Related Attacks** – *Craig Clapp (chair)*

- ❑ "Power Analysis of the Key Scheduling of the AES Candidates" *(Adi Shamir)*
- ❑ "Resistance Against Implementation Attacks: A Comparative Study of the AES Proposals" *(Joan Daemen)*
- ❑ "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards" *(Pankaj Rohatgi)*

17:30 **Reception**

- ❑ Cash bar and hors d'oeuvres

18:30-20:30 **Rump Session** – *Jim Foti (chair)*

Day 2 – Tuesday, March 23

8:00 – 9:00

- Registration, material distribution
- Coffee

9:00 **Announcement of AES3**

9:10 **Session 5: Crypto Attacks** *(Susan Langford - chair)*

- "An Observation on the Schedule of Twofish" *(Sean Murphy)*
- "Key Schedule Weaknesses in SAFER+" *(John Kelsey)*
- "Weaknesses in LOKI97" *(Vincent Rijmen)*
- "Cryptanalysis of FROG" *(David Wagner)*
- "Cryptanalysis of MAGENTA" *(Eli Biham)*

11:00 Break

11:30 **Session 6: Algorithm Observations** *(David Aucsmith - chair)*

- "DFC Update" *(Jacques Stern)*
- "Pseudorandomness and Maximum Average of Differential Probability of Block Ciphers with SPN-Structures like E2" *(Kazukuni Kobara)*
- "On the Optimality of SAFER+ Diffusion" *(James Massey)*
- "On Differential Properties of Data-Dependent Rotations and Their Use in MARS and RC6" *(Scott Contini)*
- "New Results on the Twofish Encryption Algorithm" *(Doug Whiting)*

13:00 Lunch (provided)

14:30 **Session 7: Algorithm Submitter Rebuttals and Discussion**
(Miles Smid – chair)

16:00 Break

16:30 **Future Plans and Closing** *(Miles Smid)*

17:30 Adjourn