The Second
Advanced Encryption Standard (AES)
Candidate Conference

March 22-23, 1999

Hotel Quirinale
Rome, Italy

****

PRELIMINARY 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)*

- *(3 presentations + discussion)*

11:00 Break

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

- *(4 presentations + discussion)*

13:00 Lunch (provided)

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

- *(2 presentations + discussion)*

15:30 Break

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

- *(3 presentations + discussion)*

17:30 **Reception**

- Cash bar and hors d'oeuvres

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

- *(Please contact Jim AT THE CONFERENCE if you have a topic to present. He is NOT accepting proposals until Monday, March 22.)*

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)*

- *(5 presentations + discussion)*

11:00 Break

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

- *(5 presentations + discussion)*

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