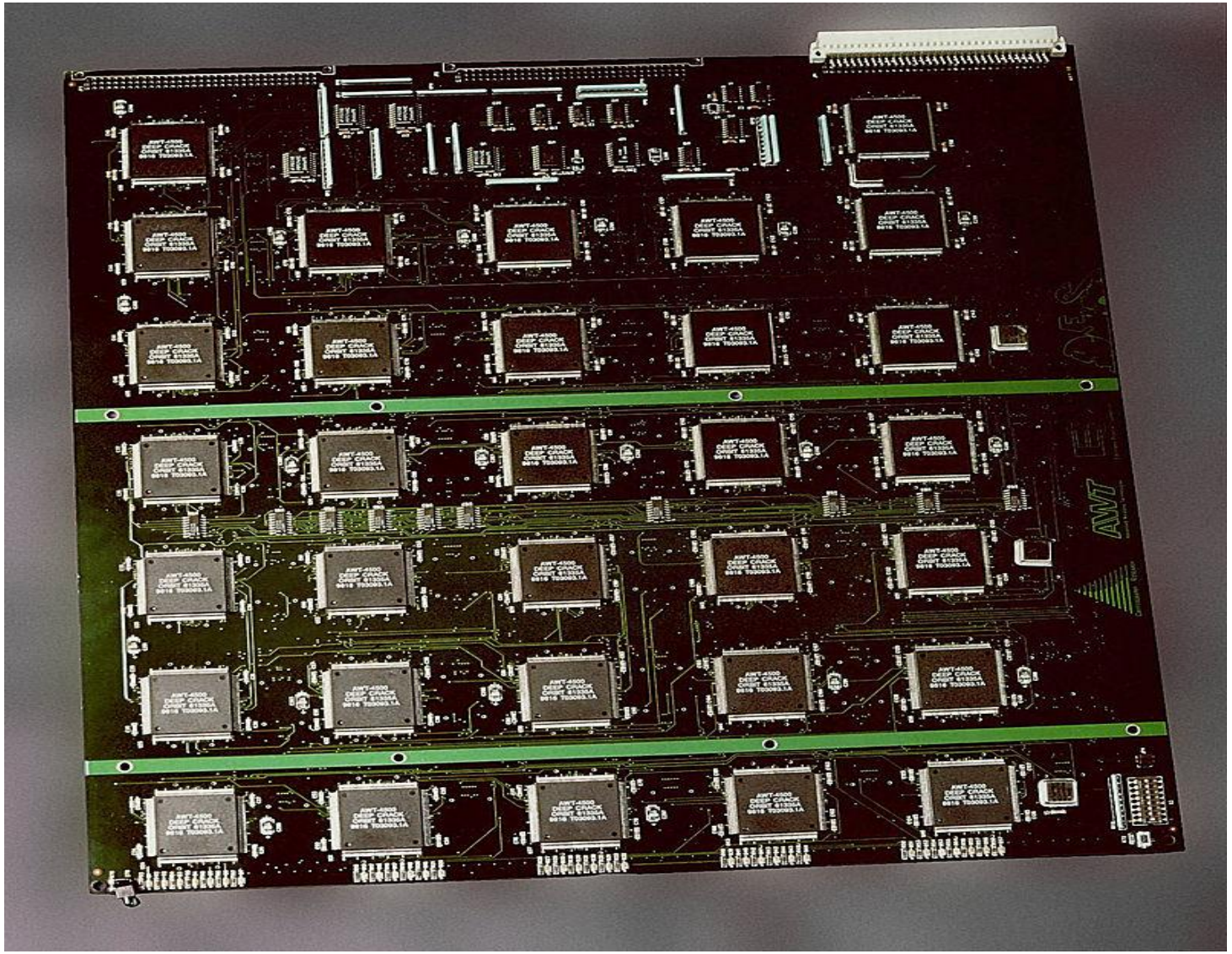
MẬT MÃ HỌC CƠ SỞ (INT1344)

Huỳnh Trọng Thưa – htthua@ptithcm.edu.vn

Gậy mật mã



DES Cracker

#62 Phil Zimmermann
PGP

Creator of the e-mail encryption program Pretty Good Privacy, which outlasted the feds who sought to make it illegal.

TOP 100
MOST INFLUENTIAL PEOPLE IN IT

Grading

- Class participation: 10%
- Lab/HW/Discuss: 20%
- Mid-Term: 10%
- Final exam: 60%

Tentative Schedule

- Week 1 *Tổng quan về Mật mã học*
- Week 2 *Cơ sở toán học của Mật mã học*
- Week 3 *Mã hóa khối, mã hóa luồng*
- Week 4 *No class (Lunar new year)*
- Week 5 *No class (Lunar new year)*
- Week 6 *Mã hóa đối xứng*
- Week 7 *Mã hóa đối xứng (tt)*
  - Lab 1 (G1)
- Week 8 *Mã hóa bất đối xứng*
  - Lab 1 (G2)
- Week 9 *Mã hóa bất đối xứng (tt)*
  - Lab 2 (G1)
- Week 10 Midterm; Hàm băm
  - Lab 2 (G2)
- Week 11 Chữ ký số
  - Lab 3 (G1)
- Week 12 PKI
  - Lab 3 (G2)
- **FINAL EXAM**

References

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996.
2. Christof Paar and Jan Pelzl, *Understanding Cryptography*, Springer Heidelberg Dordrecht London New York,2010, 382p.