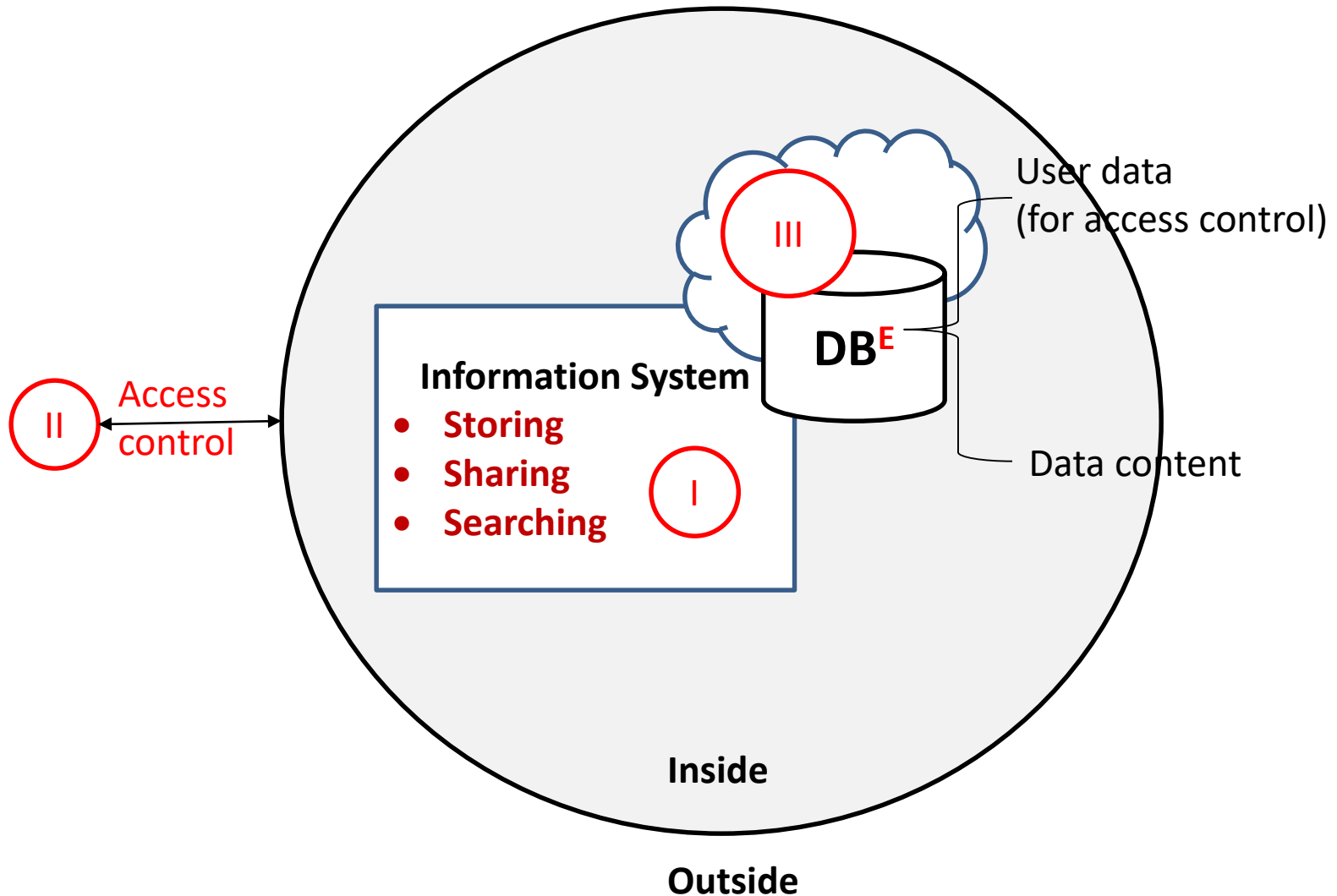


DATABASE SECURITY

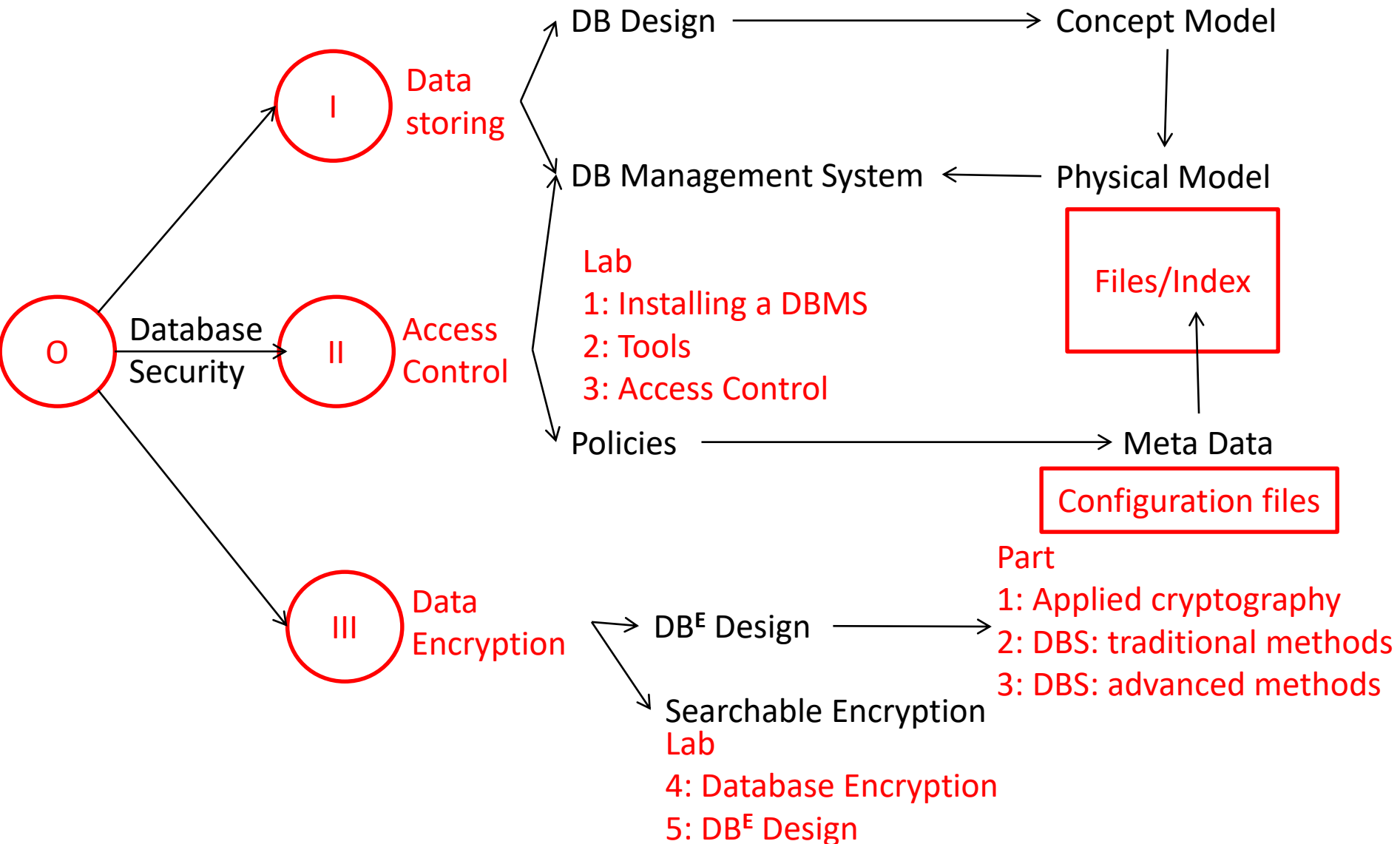
introduction

Lecture 1

Secure an Information System



Database Security



DBS Syllabus

- Part 1: Applied cryptography
 - Cryptography systems
 - Homomorphic cryptography
- Part 2: DBS – classical approach
 - Password security
 - Chinese Remainder Theorem based method
- Part 3: DBS – advanced methods
 - Secure Index / Searchable encryption
 - Database outsourcing

References

- Bùi Doãn Khanh - Nguyễn Đình Thúc, Mã hoá Thông tin: Lý thuyết và Ứng dụng, NXBLĐXH, 2004.
- Jeffrey Hoffstein – Jill Pipher – Joseph H. Silverman, An introduction to mathematical cryptography, Springer, 2008.
- Lecture Notes
- Papers