KEAMANAN INFORMASI

11. PUBLIC KEY INFRASTRUCTURE

Doni Abdul Fatah
github.com/doniaft
Universitas Trunojoyo Madura

Pokok Bahasan

01. Pengantar Keamanan Informasi

02. Pemodelan Serangan (Attack Tree)

03. Sistem Keamanan Informasi dan Internet

04. Autentikasi

05. Kontrol Akses

06. Firewall dan Intrusion Detection System

07. Network Attack

08. Kriptografi

09. Kriptografi Asimetrik

10. Biometric Authentication

11. Public Key Infrastructure

12. Protokol Keamanan

13. Malware & Computer Forensics

14. UAS

01. Keamanan Informasi

1) Public Key Infrastructure
2) Biometric Authentication
3) Contact
4) Referensi

11. Public Key Infrastructure

Public Key Infrastructure

- Pada Kriptografi Asimetrik terdapat problem dalam pendistribusian kunci publik
  - Bagaimana mengetahui apakah kunci publik Ka benar-benar milik A
  - Serangan MiM dimana attacker menukar kunci publik 2 orang yang berkomunikasi dengan kunci publik miliknya sendiri
- Kohnfelder (mahasiswa sarjana strata 1, Teknik Elektro, MIT) memperkenalkan konsep PKI (Public Key Infrastructure) Loren M Kohnfelder, ”Towards a Practical Public-Key Cryptosystem”, Bachelor Thesis, MIT, 1978

Konsep PKI

- Konsep :
  - CA (Certification Authority)
  - Digital Certificate
  - RA (Registration Authority)
  - Certification Revocation List (CRL)
- CA adalah TTP (Trusted Third Party - Pihak Ketiga Terpercaya) yang memvalidasi identitas seseorang / badan, dan mengikat (binding) identitas tersebut dengan kunci publik entitas tersebut.
- CA mengelola dan mendistribusikan Digital Certificate / Sertifikat Elektronik yang mengasosiasikan kunci publik dengan identitas pemiliknya.

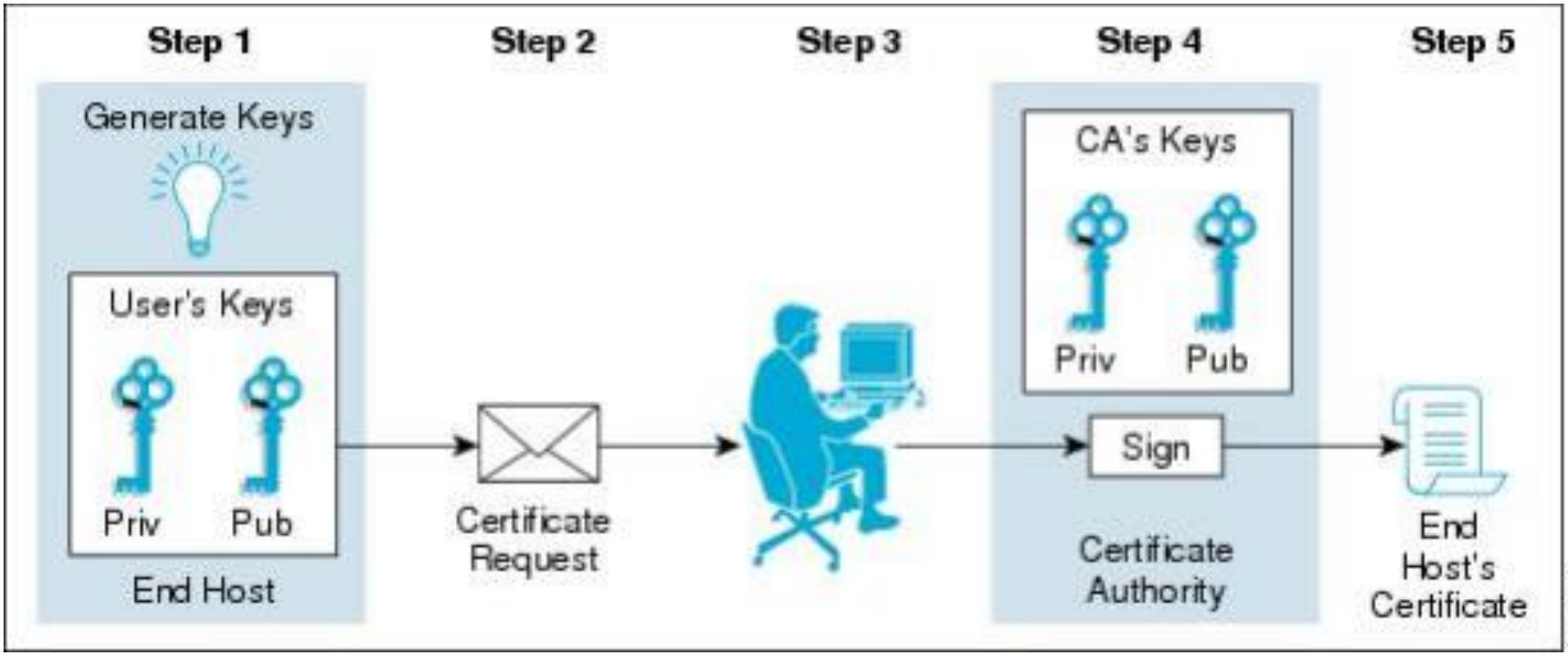
Konsep PKI

- Jika Id_a adalah identitas dan atribut-atribut yang berkenaan dengan entitas A, $\{K_{CA}, K_{CA}^{-1}\}$ adalah kunci publik dan kunci privat sebuahCA, maka sertifikat elektronik adalah :

$$\left\langle Id_a, K_a, \{h(Id_a, K_a)\}_{K_{CA}^{-1}} \right\rangle$$

- RA adalah bagian dari CA yang secara administratif membantu CA untuk memvalidasi identitas pemohon digital certificate
- CRL adalah suatu daftar berisi serial number digital certificate yang dibatalkan
- Sertifikat Elektronik (demikian terjemahannya dalam UU ITE) berstandar X.509

Proses CA


Step 1
Step 2
Step 3
Step 4
Step 5
Generate Keys
User's Keys
Priv
Pub
End Host
Certificate Request
CA's Keys
Priv
Pub
Sign
Certificate Authority
End Host's Certificate
238762

X509 Sertifikat Digital

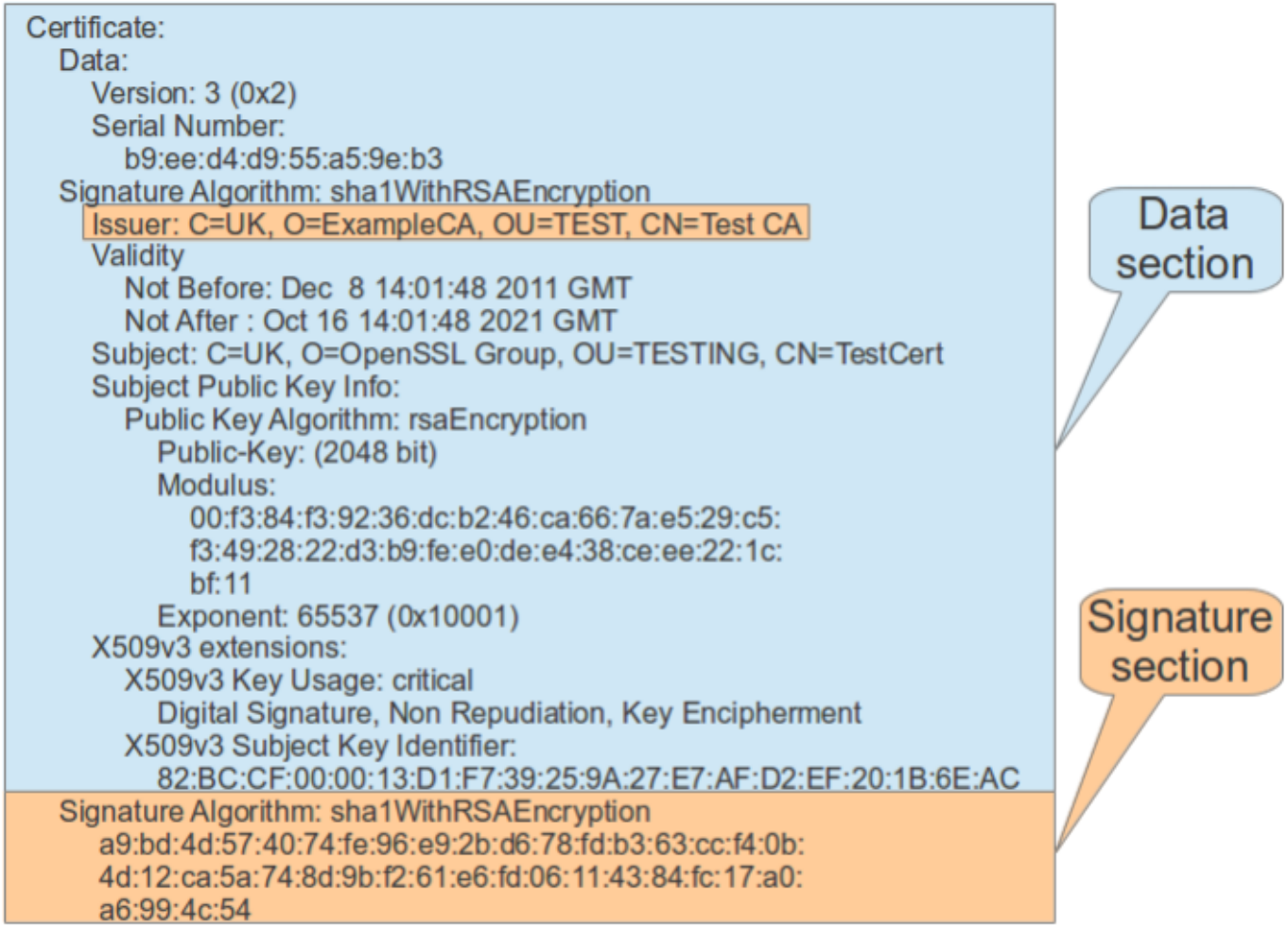


Figure 1. Anatomy of an X.509 Certificate

Proses Verifikasi Dengan DC

- CA mengeluarkan Self-Signed-Certificate (SSC CA), yaitu sertifikat elektronik yang berisi kunci publik CA KCA Pengguna mendapatkan SSC CA dengan cara yang aman (misalnya bawaan OS atau Browser, atau diambil dengan menggunakan CD-ROM)
- Asumsi : pengguna mempercayai SSC CA untuk memverifikasi DC lainnya
- Notasi : DC_a dan DC_b adalah sertifikat elektronik A dan B yang diterbitkan oleh CA dan berisi identitas masing-masing (nama, email, dll) serta kunci publiknya masing-masing (K_a, K_b)

Proses Verifikasi Dengan DC

- **Misal A mengirim email dengan konten m ke B.**

1. A mendapatkan DC_b langsung dari B atau dari LDAP CA.
2. A memverifikasi ttd elektronik CA pada DC_b dengan menggunakan K_{CA} yang terdapat pada SSC-CA, sehingga mendapatkan kunci publik K_b yang ada dalam DC_b.
3. A mengirimkan email ke B : $A \rightarrow B : \left\{ m, \{h(m)\}_{K_a^{-1}}, DC_a \right\}_{K_b}$
4. B menerima email dan mendekrip dengan kunci privatnya $\left(K_b^{-1}\right)$ sehingga mendapatkan $m, \{h(m)\}_{Ka}{}^{-1}, DC_a$
5. B memverifikasi ttd elektronik CA pada DC_a dengan menggunakan K_{CA} yang terdapat pada SSC-CA, sehingga mendapatkan kunci publik K_a yang ada dalam DC_a
6. B mendekrip tandatangan elektronik A terhadap m : $\{h(m)\}_{Ka}{}^{-1}$ sehingga mendapatkan *h(m)*
7. B memeriksa integritas m dengan *h(m)*

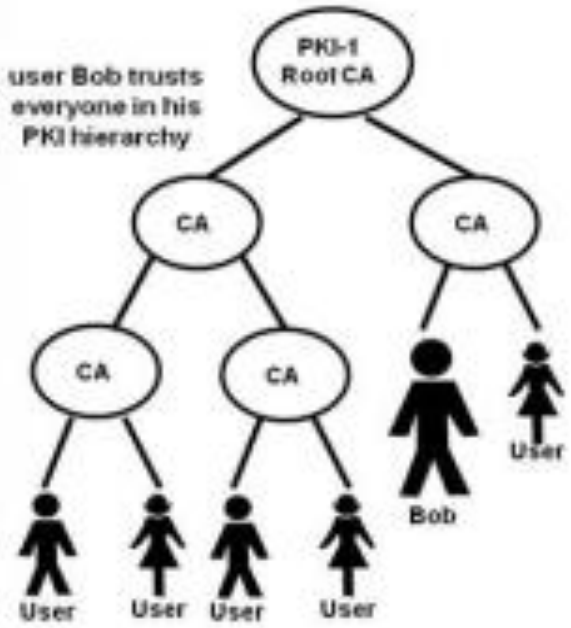
Proses Verifikasi Dengan DC

- Jika langkah ketujuh benar, maka :
  - B percaya bahwa m dikirim oleh A
  - B memastikan bahwa m tidak termodikasi selama pengiriman
  - tidak ada yang dapat membaca m kecuali B dan A (sebagai pengirim)
  - A tidak dapat mengelak bahwa dia mengirimkan email m ke B
- Jika tersedia CRL, maka entitas dapat mendownload CRL tersebut dan memeriksa apakah sertifikat elektronik dalam daftar cekal tersebut.
- Saat ini, CRL dapat digantikan dengan OCSP (Online Certificate Status Protocol) karena data lebih terkini dan realtime.

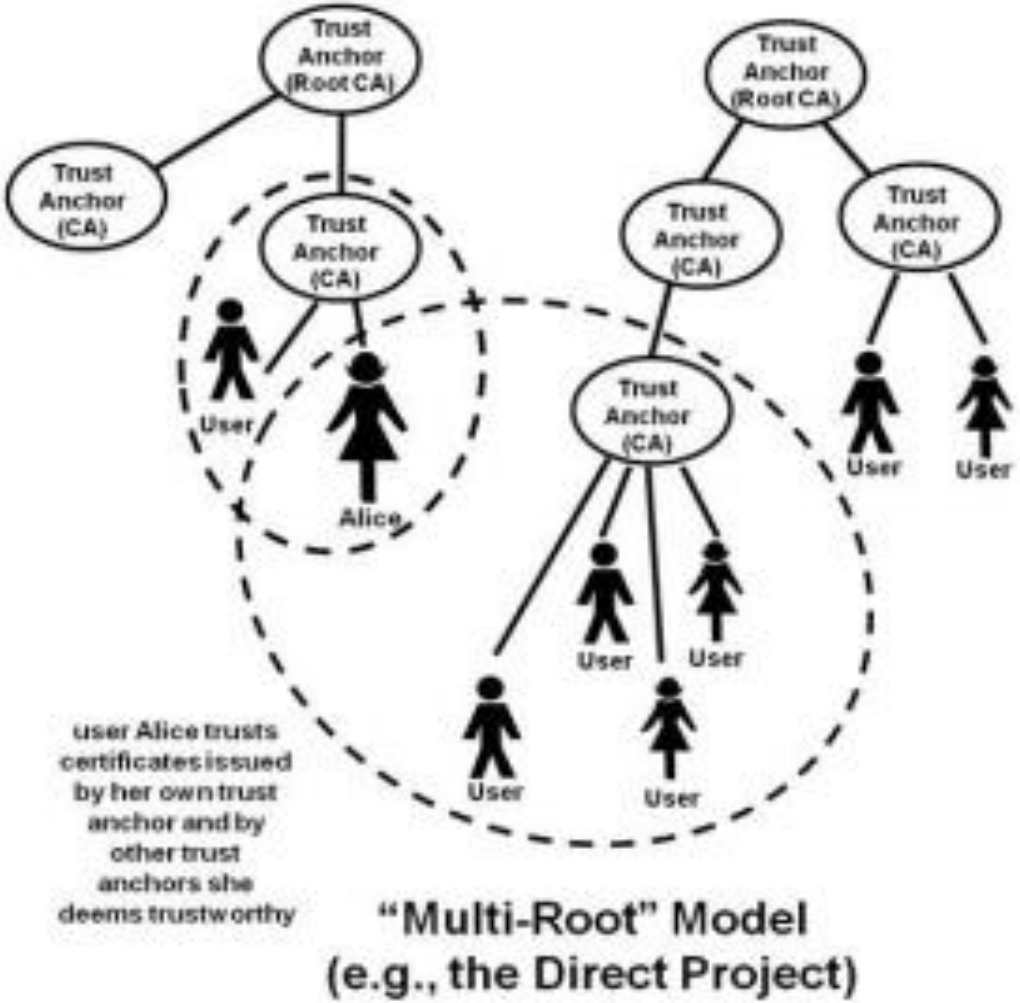
Trust Model PKI

- **Oligharchy**
  - Entitas mempercayai banyak CA
  - Browser “memaksa” untuk mempercayai banyak CA (lebih kurang ada 80 CA dalam browser saat ini)
  - User dapat menambah SSC-CA atau tidak mempercayai CA yang ada dalam browser tersebut
- **Anarchy Model**
  - Siapapun bisa menjadi CA
  - PGP (Pretty Good Privacy) Web of Trust
  - Pengguna harus memilih siapa saja yang hendak dipercaya
- **Hierarchical Model**
  - Ada satu root CA yang berada di puncak kepercayaan, setiap user hanya perlu mendapatkan SSC-RootCA
  - Root-CA menerbitkan sertifikat elektronik bagai CA - CA di bawah hierarkinya
  - CA yang berada di hirarki paling bawah akan mengeluarkan
  - DC untuk end-user
- **Hybrid Model**
  - Bebas
  - Bisa terjadi “cross-certification” antar CA untuk saling mempercayai

DC Trust Model PKI



Hierarchical PKI



"Multi-Root" Model
(e.g., the Direct Project)

Public Key Infrastructure

- CA sebagai TTP adalah solusi bagi kepercayaan terhadap DC
- CA menerbitkan : sertifikat elektronik, CRL, dan menyediakan OCSP
- Operasi CA didasarkan pada :
  - Kemampuan CA untuk tidak salah dalam menerbitkan DC (pernah terjadi di Microsoft)
  - Kemampuan CA untuk melindungi private-key nya

3) Kontrak Perkuliahan

a) Tata Tertib
b) Contact
c) Referensi

Tata Tertib Perkuliahan SI4B

- Masuk sesuai jadwal 15.25 WIB, Toleransi keterlambatan adalah 20 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4C

- Masuk sesuai jadwal 09.15 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Tata Tertib Perkuliahan SI4D

- Masuk sesuai jadwal 12.45 WIB, Toleransi keterlambatan adalah 15 menit.
- Pakaian bebas rapi berkerah, bersepatu.
- Segala macam bentuk ijin ketidakhadiran diharuskan dengan alasan yang jelas
- Setiap mahasiswa dilarang mencontek dalam pengerjaan tugas dan ujian, jika terjadi maka pengerjaan tugas dan ujian akan dikurangi 20% atau Gugur.
- Setiap mahasiswa dilarang melakukan tindakan plagiat atas pengerjaan tugasnya, jika terjadi maka pengerjaan tugas akan dikurangi 20% atau Gugur.
- Setiap mahasiswa wajib mengerjakan ujian dan tugas baik tugas mandiri ataupun berkelompok.
- Wajib untuk bertutur kata yang sopan dan santun didalam kelas dan berpakaian rapih dan sopan

Proyek : Kelompok
dibuat 2 s.d 4 Mahasiswa

- Membuat aplikasi sederhana dengan fokus **Keamanan Informasi dalam Penggunaan** Aplikasi/berInternet
- **Tahapannya :**
  - Penentuan Studi Kasus
  - Membuat aplikasi Login Spoofing Attack
  - Dalam aplikasi Login Spoofing Attack untuk pemberian passwordnya di lakukan dengan menggunakan teknik Kriptografi (enkripsi) dengan menggunakan enkripsi asimetris
  - Untuk memecahkan enkripsi tersebut maka dilakukan deskripsi dari enkripsi tersebut.
  - Untuk Aplikasi boleh Web atau Desktop, sesuai yang dikuasai.
  - Pembuatan Laporan atau Dokumentasi.
- **Poin penilaian:** Aplikasi, Dokumentasi, Presentasi.

5) Contact

Contact

- Bahan Kuliah : github.com/doniaft
- Email : doniaft@gmail.com
- WA/Telegram :
- Komting Keamanan Informasi
  - SI4C : Yusril : 0856 5509 5641
  - SI4D : Ikrom : 0852 3027 9767
  - SI4B :
    - Rahma : : 0852 5707 1554
    - Adi : 0899 3616 728

6) Referensi

Referensi (1)

- Anderson, Ross, “Security Engineering”, First Edition, Wiley, 2001, tersedia dalam e-Book : URL: http://www.cl.cam.ac.uk/~rja14/book.html
- Menezes et.al, “Handbook of Applied Cryptography”, Fifth Edition, CRC Printing, 2001, tersedia dalam e-Book URL: http://cacr.uwaterloo.ca/hac
- Bishop, Matt, “Computer Security: Art and Science”, Addison Wesley, 2002
- Stinson, Douglas R, “Cryptography: Theory and Practice”, CRC Press, 1995
- Electronic Frontier Foundation, “Cracking DES”, O'Reilly, 1998
- Stamp, Mark, “Computer Security: Principles and Practices”, Willey, 2011
- Eric Cole, Ronald Krutz, and James W. Conley, “Network Security Bible”,
- Wiley Publishing, Inc., 2005.
- Matthew Strebe, “Network Security Foundations”, Sybex, 2004.
- Chris McNab, “Network Security Assessment”, O’reilly, 2008.
- James D. McCabe, dkk, “Network Security Know It All”,Morgan
- Kaufmann, 2008.
- Ibisa, “Keamanan Sistem Informasi”, Penerbit Andi, Yogyakara, 2011