PB173 - Tématický vývoj aplikací v C/C++ (podzim 2012)

Skupina: Aplikovaná kryptografie a bezpečné programování

https://minotaur.fi.muni.cz:8443/pb173_crypto

Petr Švenda, *svenda@fi.muni.cz*
Konzultace: G.201, Pondělí 16-16:50

Some cryptography trivia

Symmetric vs. asymmetric cryptography

- Both can be used to do most of the tasks
  - you often have choice with some limitations
  - there are exceptions and some uses impractical
- Symmetric cryptography
  - both communicating parties shares same single key
  - advantage: fast, short key lengths (~16B)
  - disadvantages: one party can mimic other one
- Asymmetric cryptography
  - one party A generates private and public key
  - what is encrypted by private can be decrypted by public and vice versa
  - private is kept secret to A, public is distributed to all other B
  - advantage: B cannot mimic A (digital signatures)
  - disadvantages: slow, long keys (>128B)

DES and AES

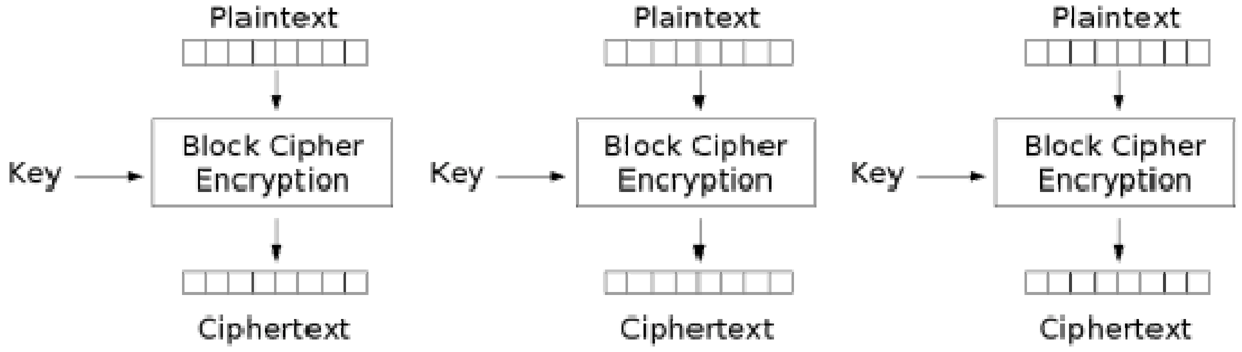
- Both are
  - symmetric cryptography algorithms
  - and block ciphers
- DES, from 1976
  - 8 bytes block, 56 bits key
  - insecure key length (DES cracker)
  - 3DES – special mode for DES, still secure, but slow
    - 112/168bits key, Encrypt(Decrypt(Encrypt(M)))
- AES, from 2002
  - 16 bytes block, 128 – 256 bits key
  - secure, fast, prefer to DES

Block vs. stream cipher

- Stream ciphers produces key stream
  - generate key stream long enough
    - can be produced in parts, e.g., few bytes
  - xor key stream with data in per byte manner
  - can pre-compute stream for data bursts
  - key is not data-dependent
  - be aware of key stream reuse
- Block cipher process input data in blocks
  - take one block (typically 16 bytes)
  - encrypt the block (e.g., by AES or DES)
  - take next block and repeat again
  - Counter mode can simulate stream cipher via block cipher

Mode of cipher usage - ECB

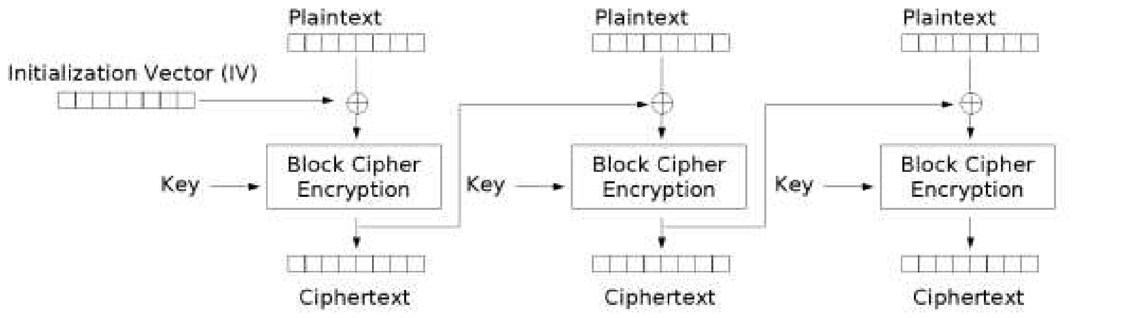
- ECB (Electronic Code Book mode)
  - used for block ciphers
  - processing of one block does not influence others
- Main problem
  - same data with same key result in same ciphertext
  - attacker can build code book



Electronic Codebook (ECB) mode encryption

Mode of cipher usage - CBC

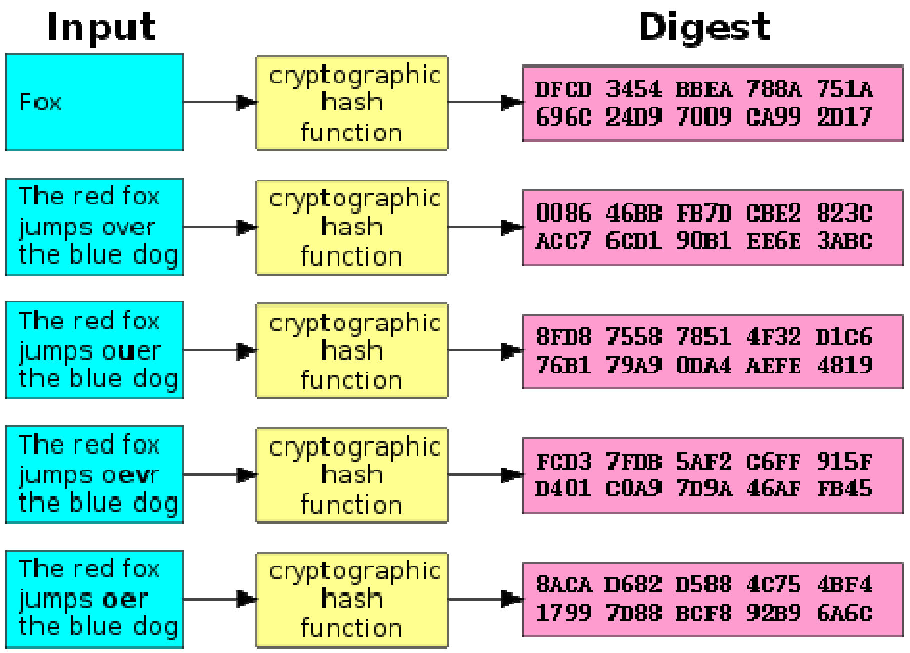
- CBC (Cipher Back Chaining mode)
  - used for block ciphers
  - previous cipher block is xored with next plaintext
  - prefer before ECB
- Problem
  - Initialization vector must be somehow shared
  - (random first block



Cipher Block Chaining (CBC) mode encryption

Cryptographic hash functions

- Function transforming long input M into fixed output D
  1. fast to compute D from M
  2. infeasible to find M from D
  3. infeasible to find for given M another M’ with same resulting D
  4. infeasible to find any pair M’ != M with same resulting D


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

MD5, SHA-1, SHA-2, SHA-3

- MD5
  - 128 bits output
  - collision exists and can be found in few seconds!!
  - insecure, do not use
- SHA-1
  - 160 bits output
  - not broken yet, but will be in close future
- SHA-2
  - 225 – 512 bits output
  - secure, prefer to SHA-1
- SHA-3
  - new competition just running, 5 candidates remain
  - http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo

MAC vs. digital signature

- Both provide robust protection against data modification
- MAC is based on symmetric cryptography
  - Message authentication code
  - both parties must know same secret key
  - protection only against external attacker
  - typically encrypt then MAC (MAC over ciphertext)
- Digital signatures on asymmetric cryptography
  - only one party knows private key
  - others can just verify it

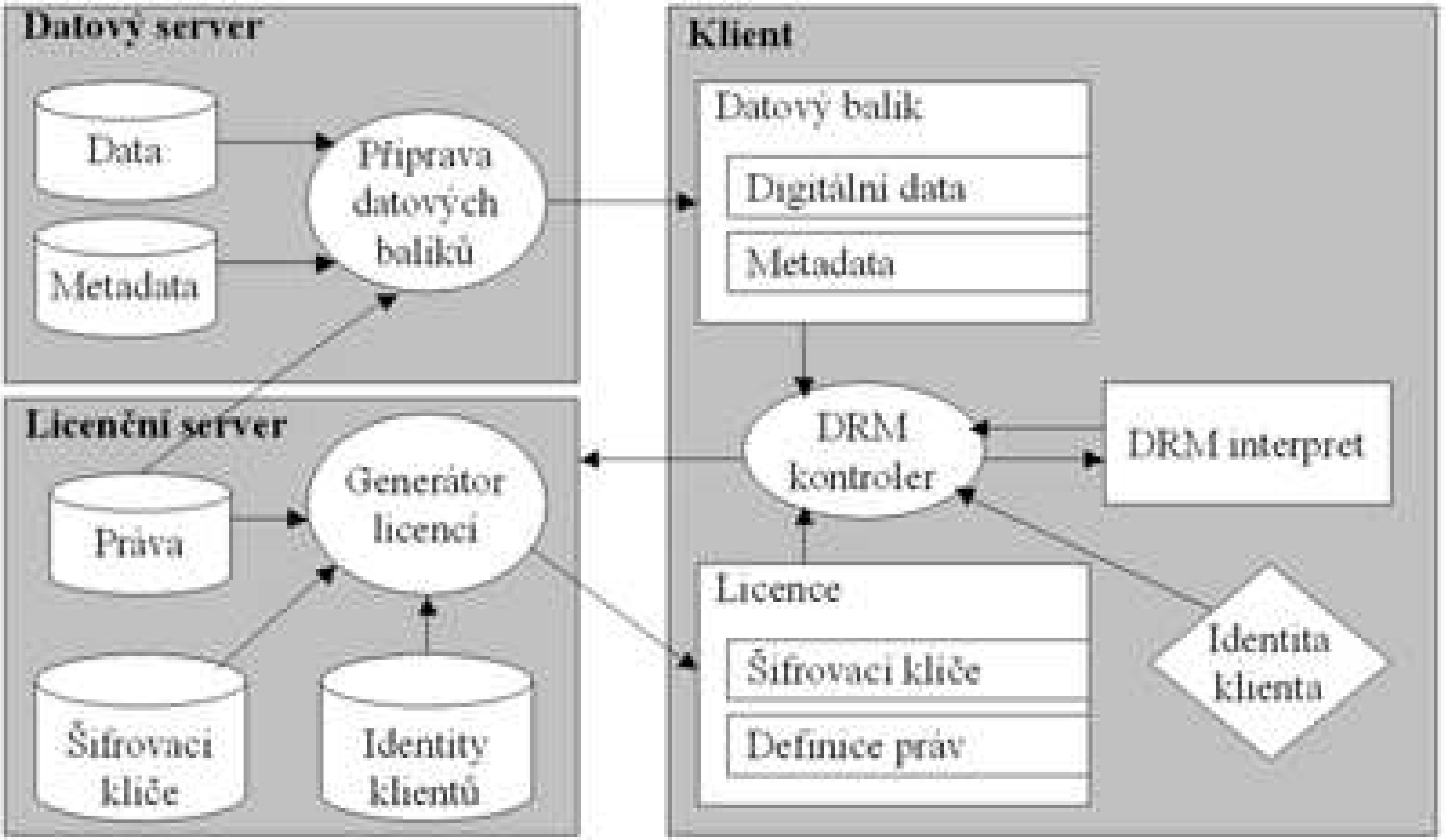
Rozdělení do týmů

- 2-3 osoby
- Společná práce, ale každý prezentuje svůj přínos
  - prezentace na každém dalším cvičení
  - resp. za 14 dni při absenci
- Rozdělení teď!
  - TODO týmy

Commented homework

- Commented codes available in IS repository
- Learn from others

Digital Rights Management (DRM)



Practical assignment

- Create specification for DRM architecture
- Functional requirements
  - involved parties and logical entities
  - format of data packets exchanged between parties
  - requirements for storage of data
- Security requirements
  - what keys will be used (symmetric/asymmetric)
  - who own which key?
  - algorithms, modes and key lengths used
  - who will have access to what data?