Baze podataka II
Modul 13 – Jezik SQL

Napredne teme

Enkripcija, forenzika i DaaS

Summary

- **Enkripcija podataka**
- **Prikupljanje digitalnih dokaza**
- **DaaS**

Lekcija 1: Enkripcija podataka

- **How to speak crypto?**
- **Quick example**
- **SQL Server encryption hierarchy**
- **Symmetric key column encryption**
- **Additionaly cryptographic features**

How to Speak Crypto?

- **encryption** is the process of transforming [information](#) (referred to as [plaintext](#)) using an [algorithm](#) (called a ciphertext) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a [key](#). The result of the process is encrypted information (in cryptography, referred to as [ciphertext](#)).
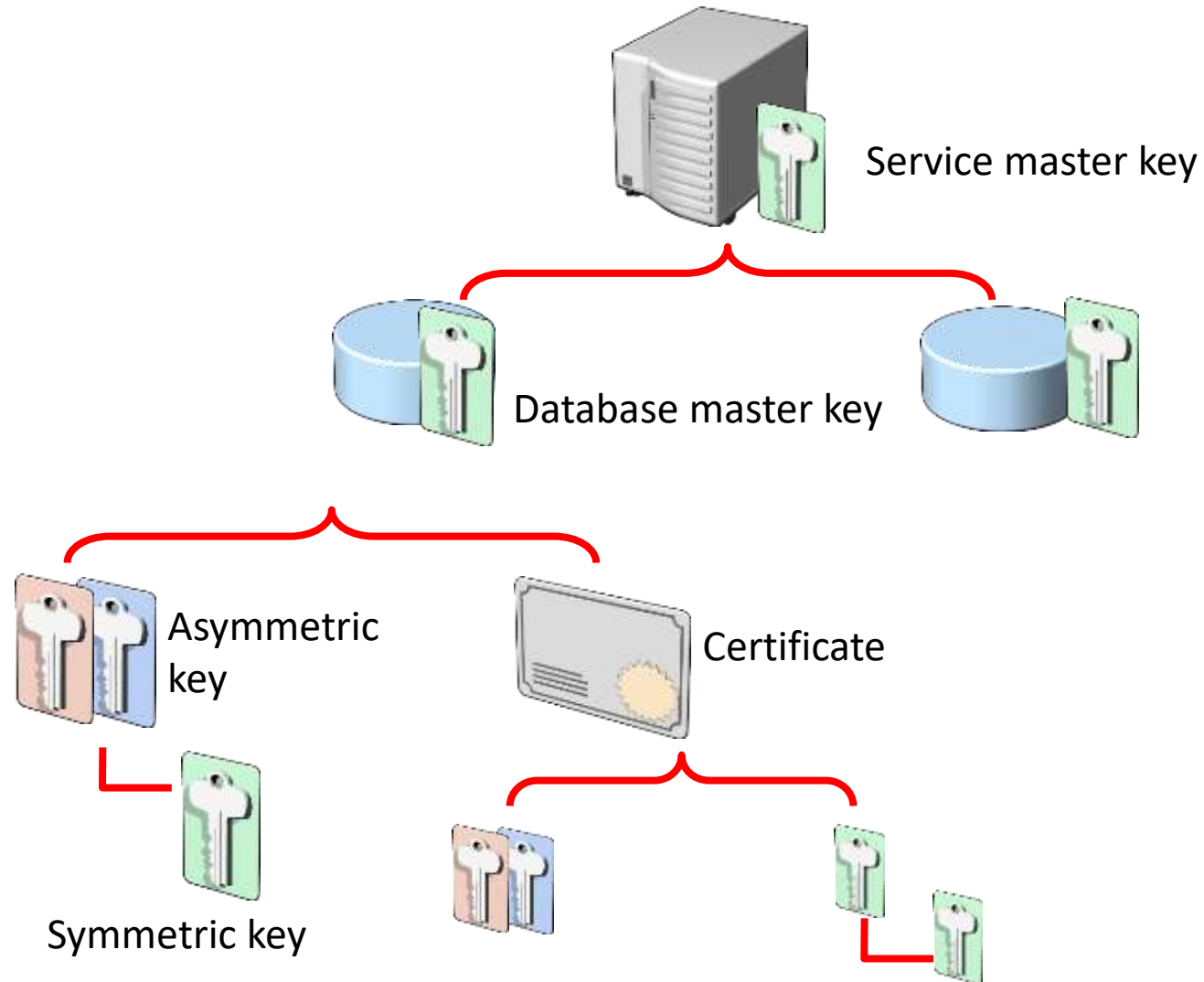
- Wikipedia

Quick example

Plaintext: Baze podataka

Ciphertext:

0x00E54815CF1CD2765D1B2392604E2E99010
00000B557EBD1C9C2E89B93D530D54880E40
B6131CECFACF55B887DD35AC5ECE2D739E43
7B2D8120225A18CEA96B34B3793A9

SQL Server encryption hierarchy

Service master key

Database master key

Asymmetric key

Certificate

Symmetric key

Symmetric key column encryption

- **Symmetric Keys are created in a database and they are always in that database**
- **What can you encrypt/decrypt?**

    - Data in tables (column level)

- **Encryption require an additional CPU load from their use.**
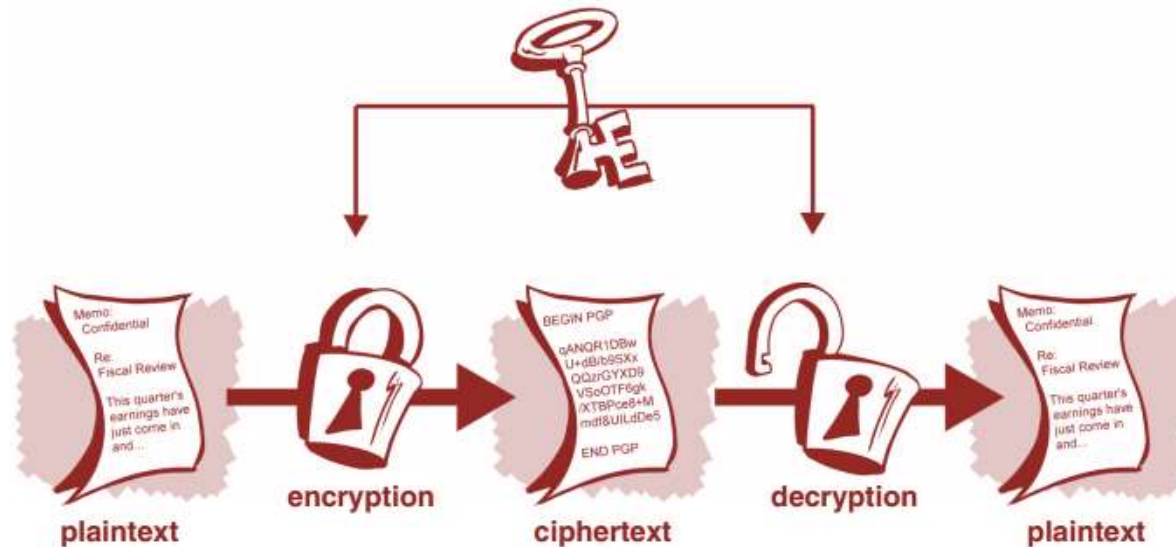
Additionaly cryptographic features

- **Asymetric encryption**
- **Transparent Data Encryption – TDE**
- **Backup encryption**
- **Always encrypted**

Lekcija 2 : Digital evidence collecting

- **Computer crime**
- **Digital forensics**
- **Phases of digital forencis**
- **Access control**
- **DDL trigger**
- **DML triggers**
- **Anti-tampering**

Computer crime

- **Computer crime is activity where computer is: resource, service, tool, target or place of criminal act.**

- **Goals?**

  - Electronic fraud

  - Identity hijacking

  - Interferences of within the data

  - Unauthorized access;

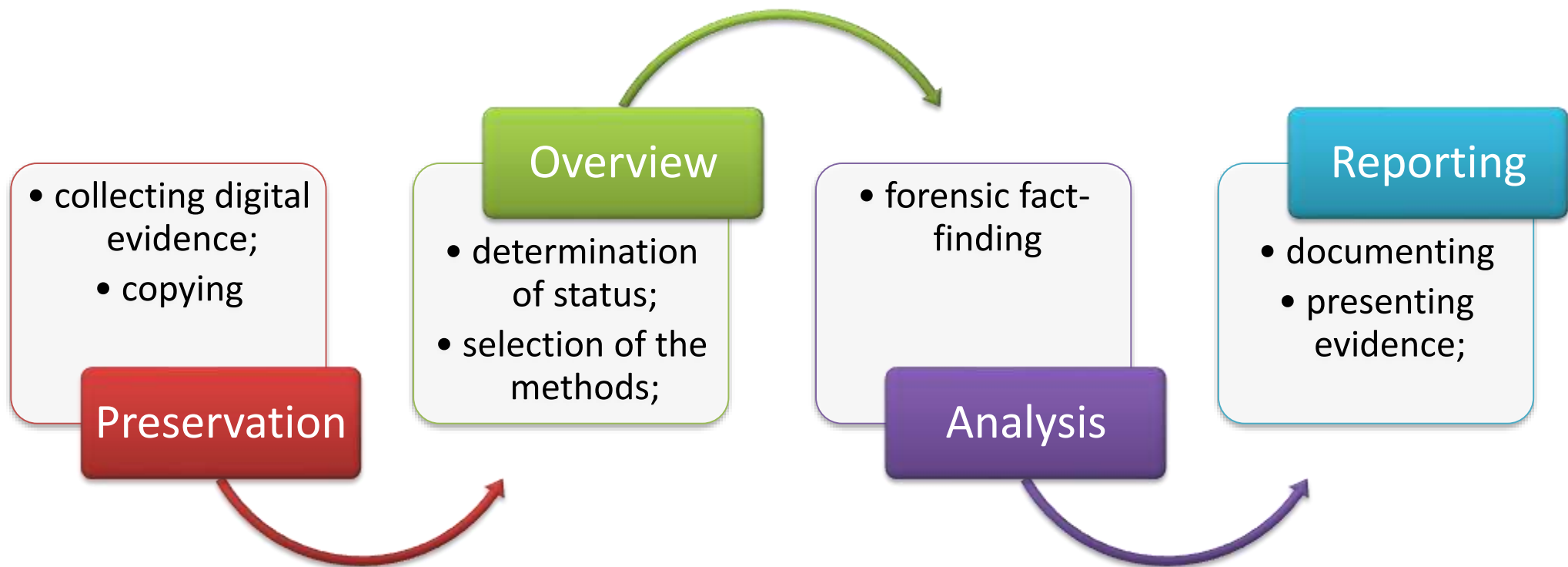 - Network interceptions;

  - ...

Digital forensics

- ...is a part of the investigation, which involves the scientific analysis: the media / storage devices and / or devices for data processing;
- Servers, PC, laptop, tablet, mobile devices, storage media...

- ... with the aim of finding traces of the activities that led to the crime.

Phases of digital forencis

Preservation
- collecting digital evidence;
- copying

Overview
- determination of status;
- selection of the methods;

Analysis
- forensic fact-finding

Reporting
- documenting
- presenting evidence;

© Jasmin Azemović 2016

Access control

DDL triggers

- **Server and database levele events**
- **Accompanied by changes in the scheme of objects**
  - CREATE, ALTER, DROP;
- ***Eventdata* function collects data for the DDL event;**
 - The output is a collection of data in XML format

DML triggers

- **DML operations are much more frequent in the DB;**
  - INSERT
  - UPDATE
  - DELETE
- **To gather information on the event types are used AFTER triggers;**
  - Unlike the DDL, DML triggers were connected to the table;
- **Performance issues;**
  - No need to put trigger on all tables;
  - The problem can be solved by generic CLR triggers

Anti-tampering

- **One of the methods**
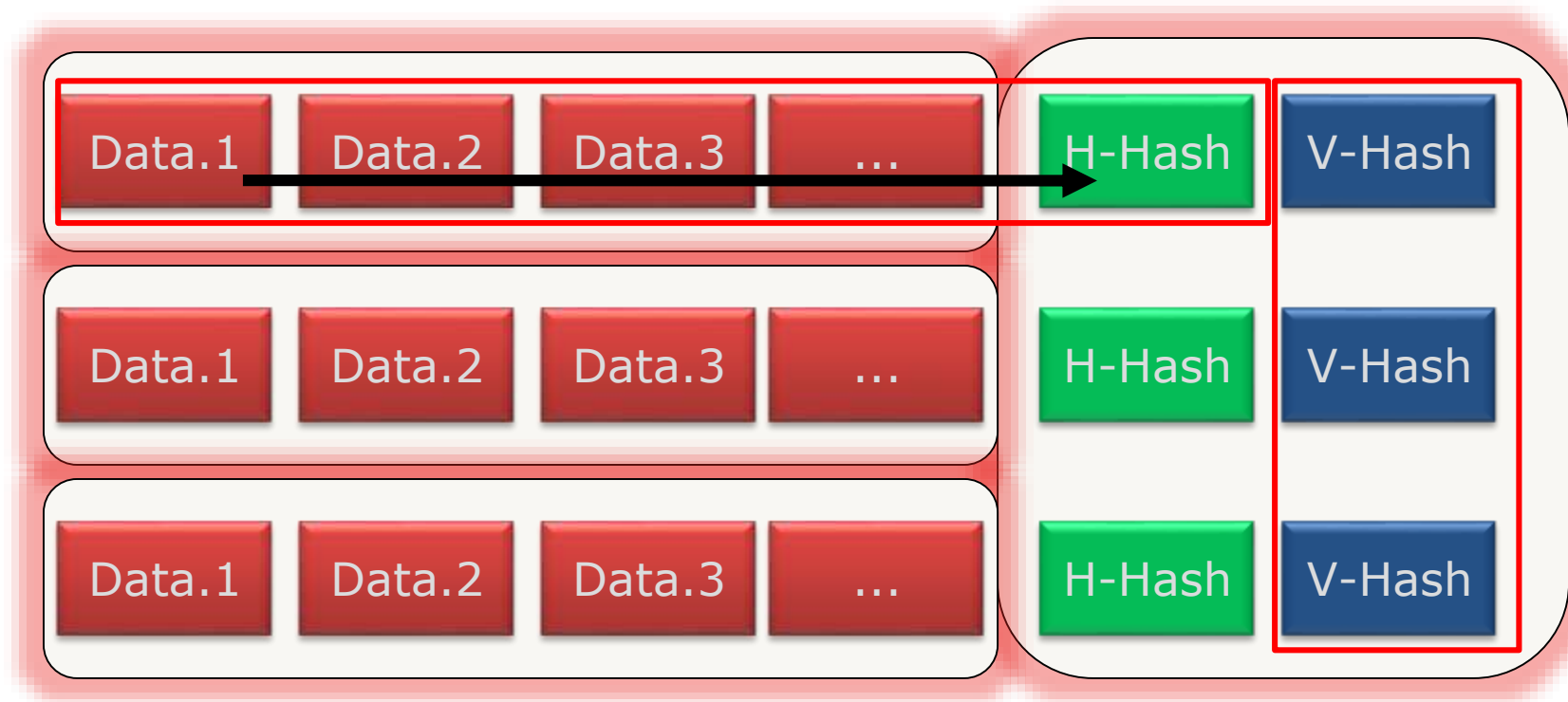
Lekcija 3 : DaaS

- **Azure introduction**
- **SQL Azure...what it is?**
- **Three different ways**
- **Some facts**

16 regions worldwide

SQL Azure...what it is?

- The **SQL** database as a service offering on Azure (OLTP).
- **Fully managed by MS as part of Azure.**
- It's not a full instance. Many features that you're used to don't exist because it's fully managed.
- At this point different then SQL Server 2014 on premise

What is SQL Azure Database?
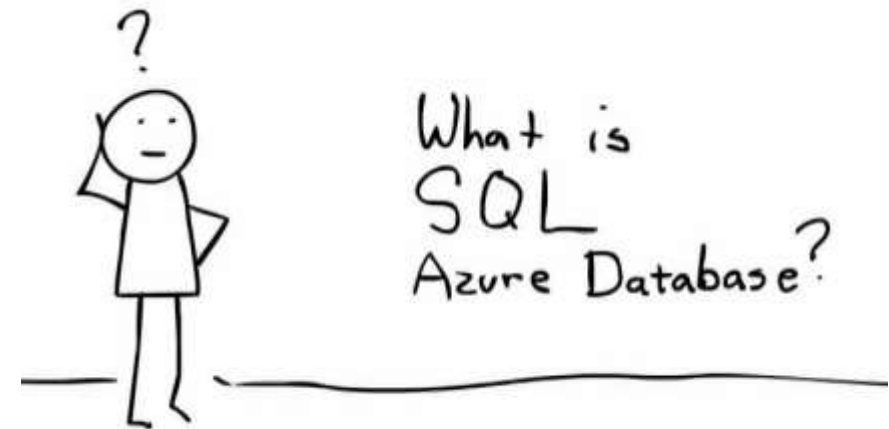
Three different ways

SQL Server

- Raw iron

SQL Server in IaaS

- Virtualized Machine

SQL Database – PaaS - DaaS

- Virtualized Database

Some facts

- **Good solutions for start-up's**
  - Small and medium size of business
- **Initial cost far beyond of „raw iron"**
- **Security, HA, is great**
- **Location of data and privacy can be issue**
  - Private cloud can fix this

Pitanja