Protecting Sensitive Data with Encryption

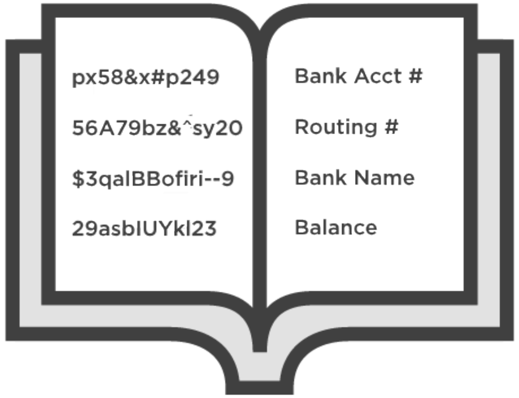
Russ Thomas
DATABASE MANAGER

@sqljudo www.sqljudo.com

Encryption

Access controls protect entry points

Encryption protects actual data within

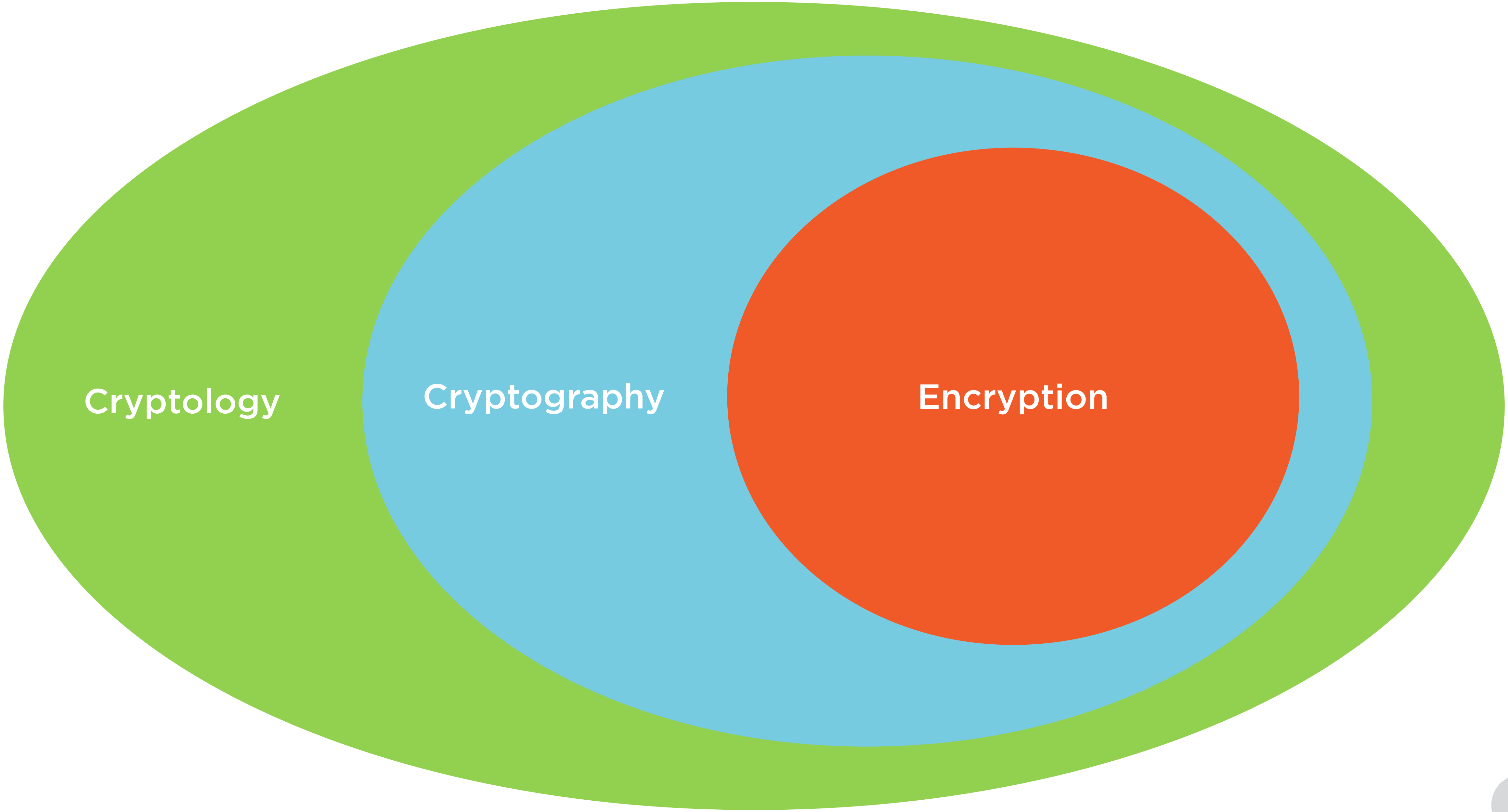


Achieved by making data seemingly useless

Data is not meaningful until decrypted

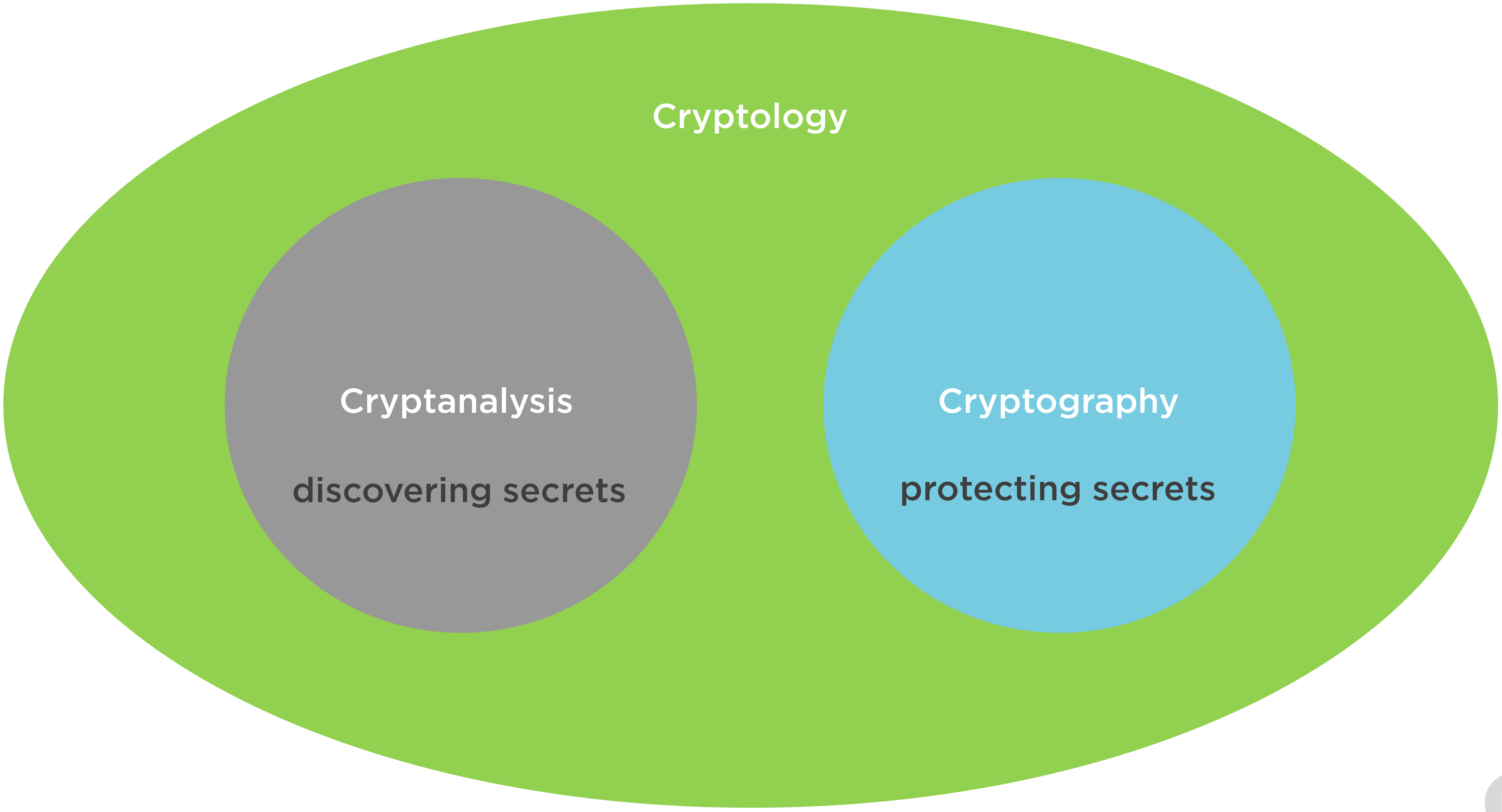
Module 4

1. Encryption and Related Topics
2. Keys and Passwords
3. Symmetric and Asymmetric
4. Encryption Algorithms
5. Certificates, Layers, and Hierarchy
6. Key Management
7. Demos and Best Practices


Cryptology
Cryptography
Encryption

Requirements of encryption:

- Hide data from individuals with or without access to the data
- Data has to be recoverable to have meaning



Cryptology

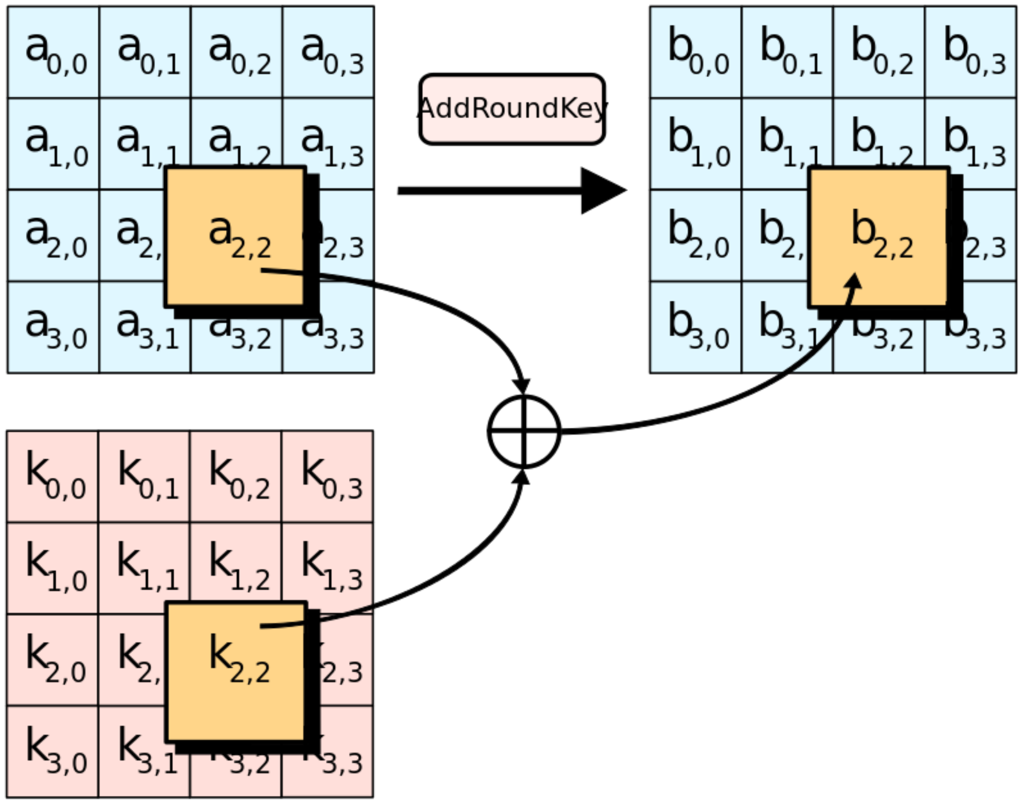
Cryptanalysis

discovering secrets

Cryptography

protecting secrets

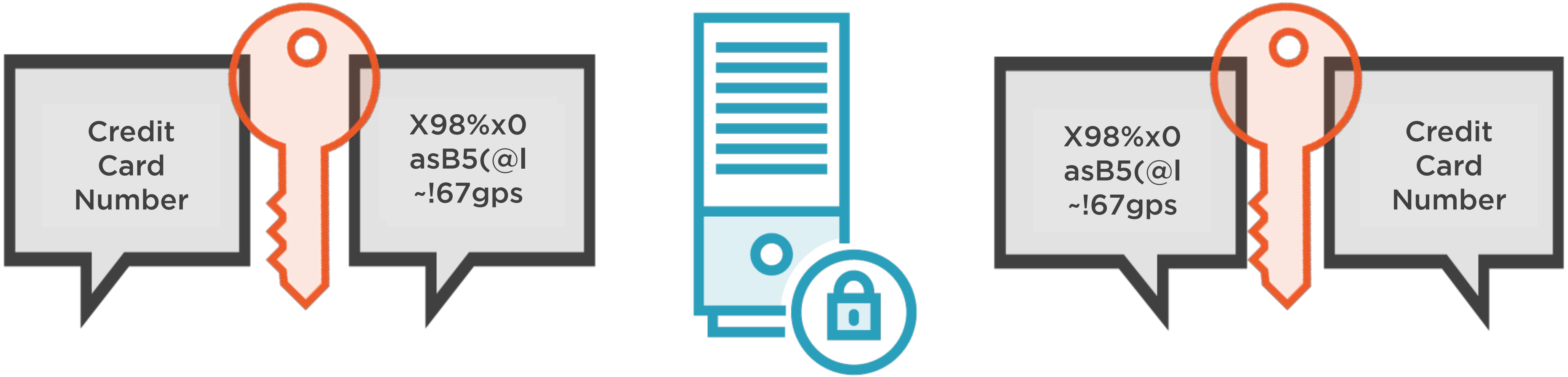
Advanced Encryption


AddRoundKey
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

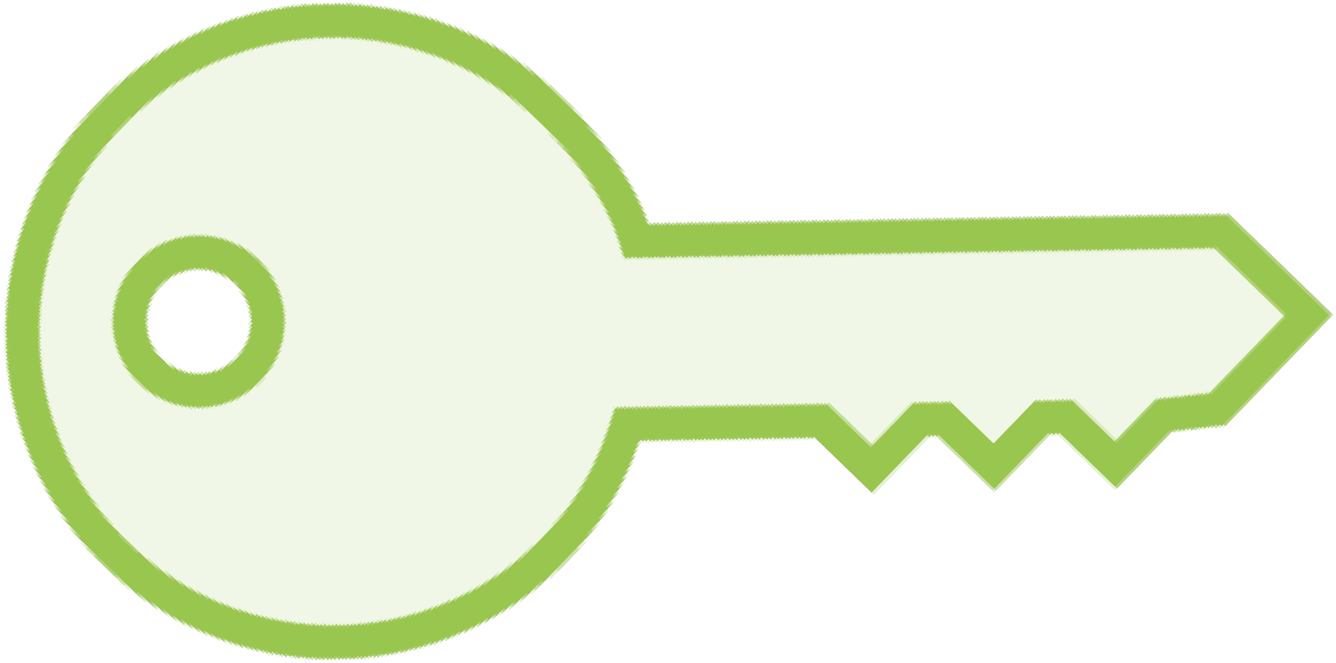
Symmetric Encryption

Asymmetric Encryption

Encryption Concept



Encryption Keys Are Critically Sensitive



A constant threat to encryption is increasingly complex attacks that discover the data without the key

The development of increasingly resilient encryption algorithms is constantly under way

Data protected by complex algorithms require more resources to store, manage, and maintain

There are many algorithms supported by versions prior to 2016

SQL Server supports AES 128, 192, and 256

AES is recommended and used by the US federal government in secret and some classified areas

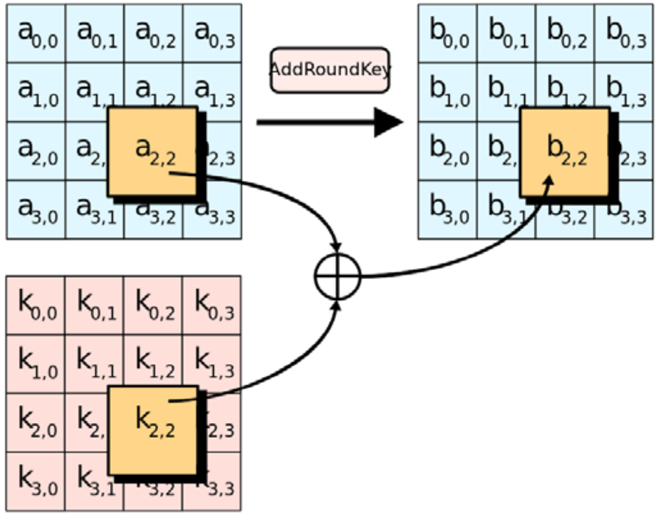
Algorithm selection best practice:

Begin with levels required by your compliance commitments

Go with the most secure keys your environment permits

Demo

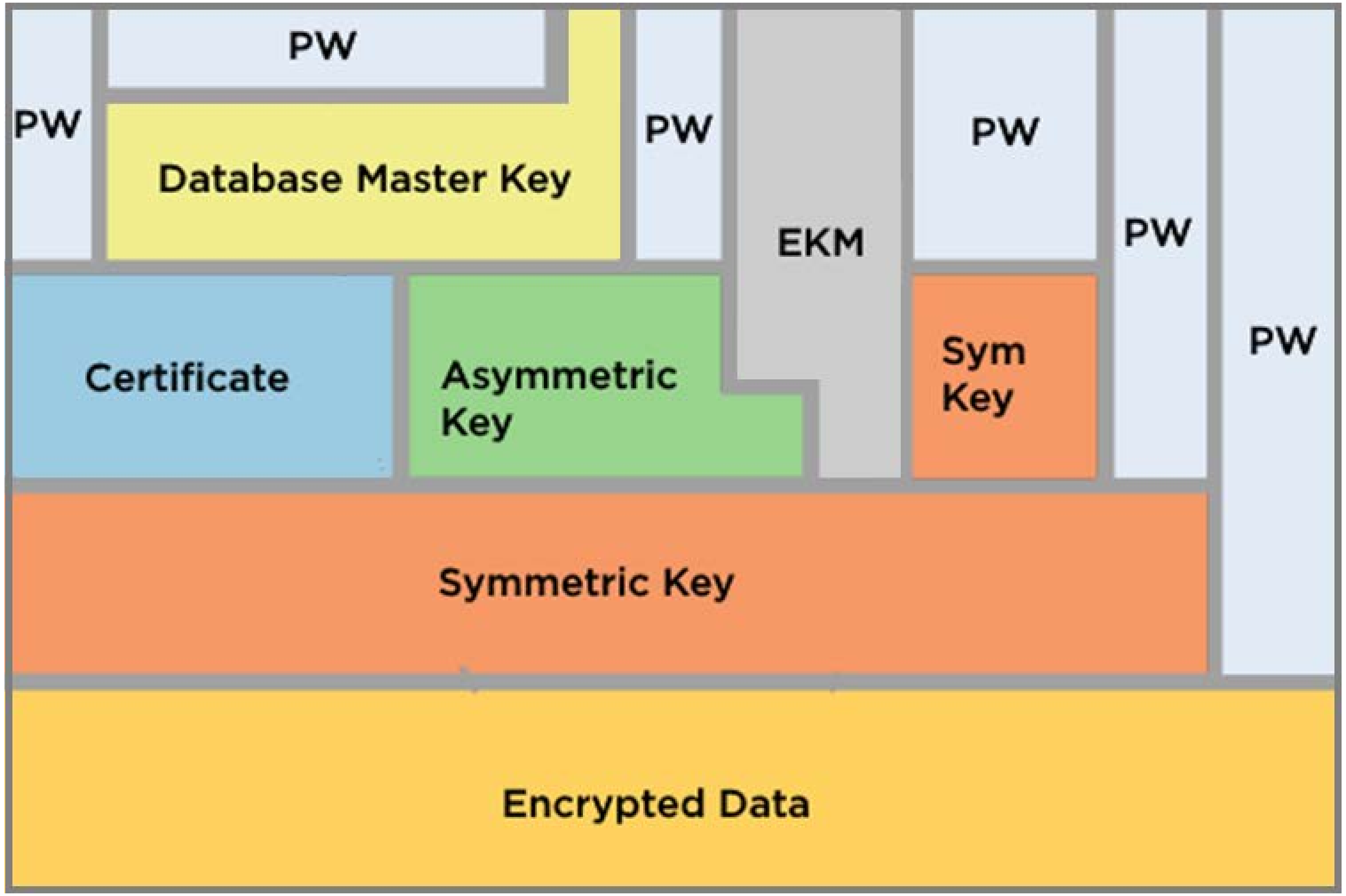
Key Management and Protection

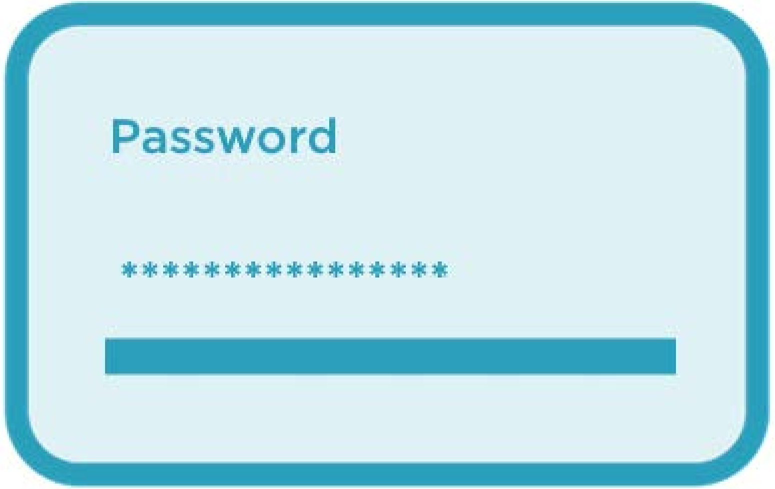


Advanced Encryption

Encryption Key

SQL Server Encryption Hierarchy





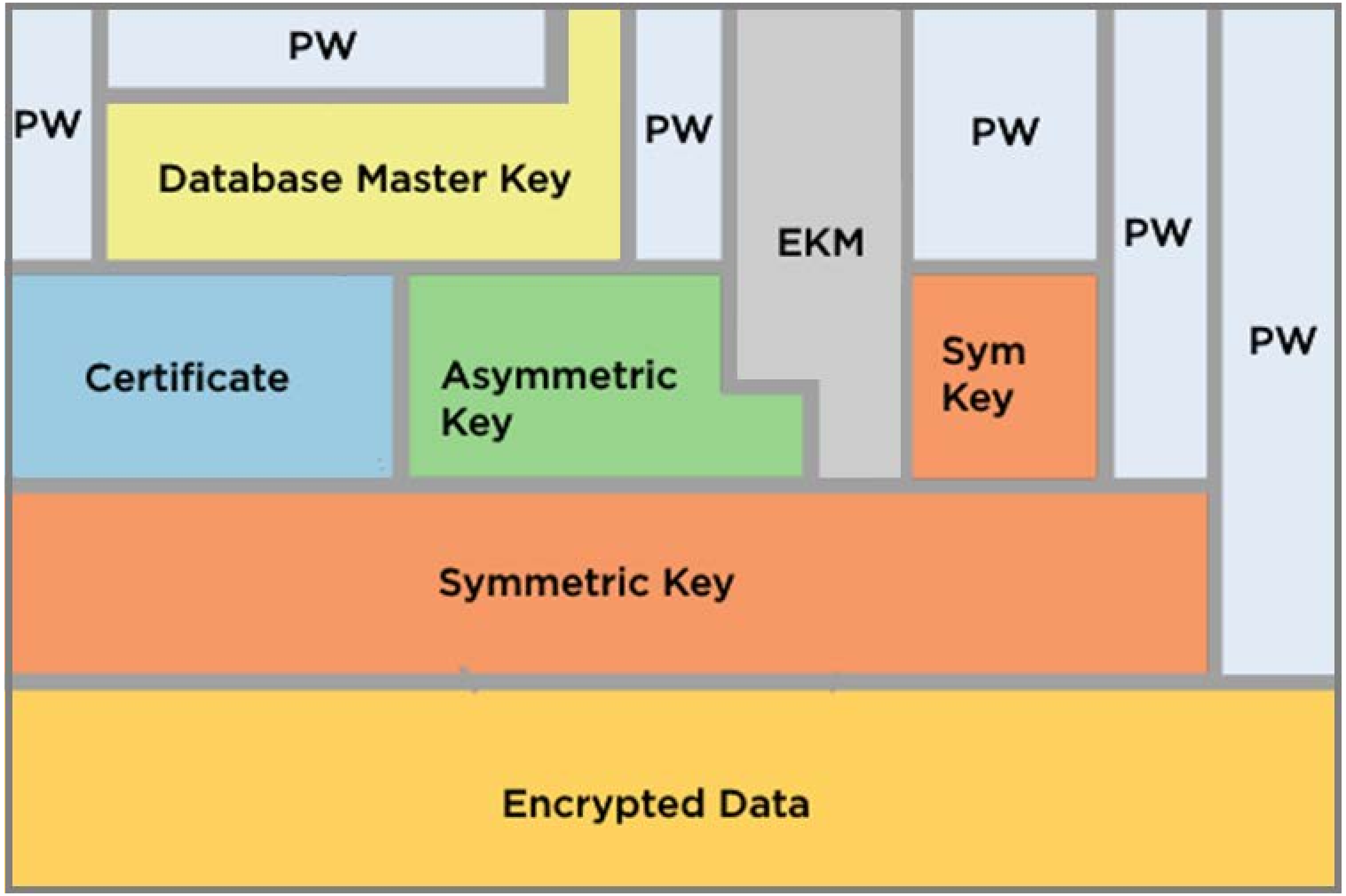
Simple Password Problems

- Easy to brute force
- Easy to pass around
- Easy to lose

Solution

- Minimize necessity of use
- Make random and complex

SQL Server Encryption Hierarchy



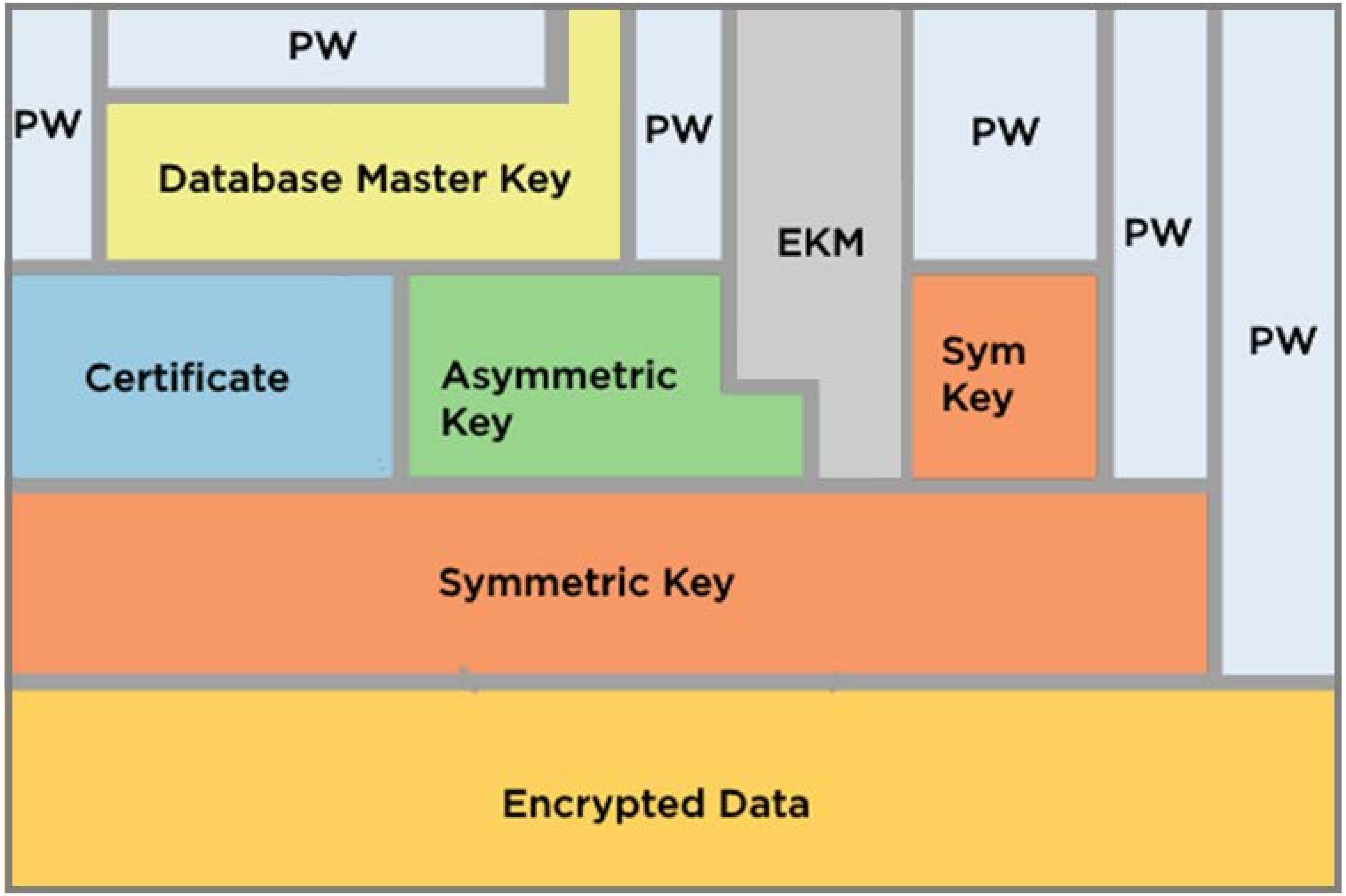
Certificates

Can be provided by trusted 3rd party

Can be generated internally

Can be public or private

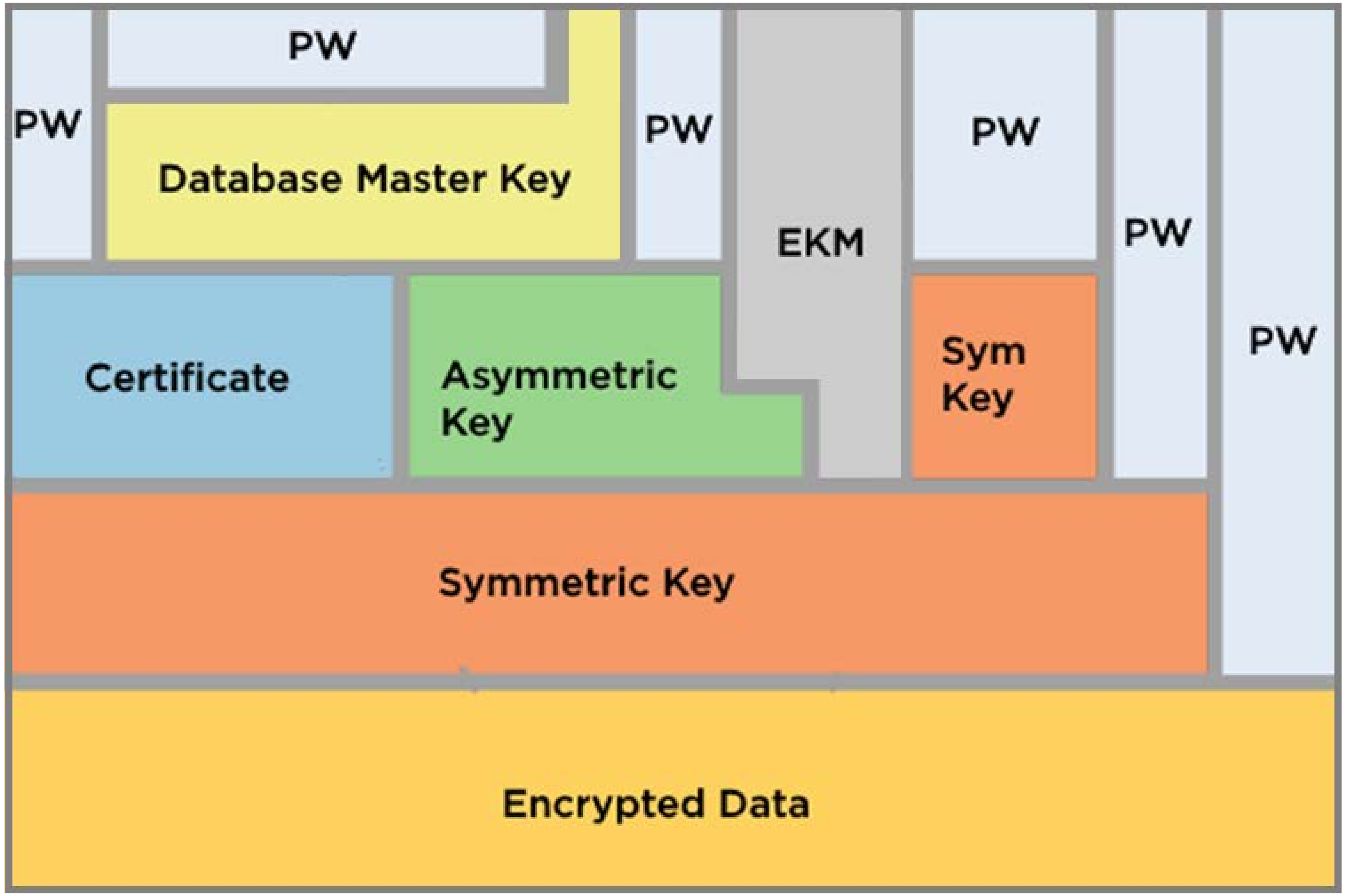
SQL Server Encryption Hierarchy



Back up your top level keys !!

A lost key means lost data !!

SQL Server Encryption Hierarchy



Strengths of using an EKM:

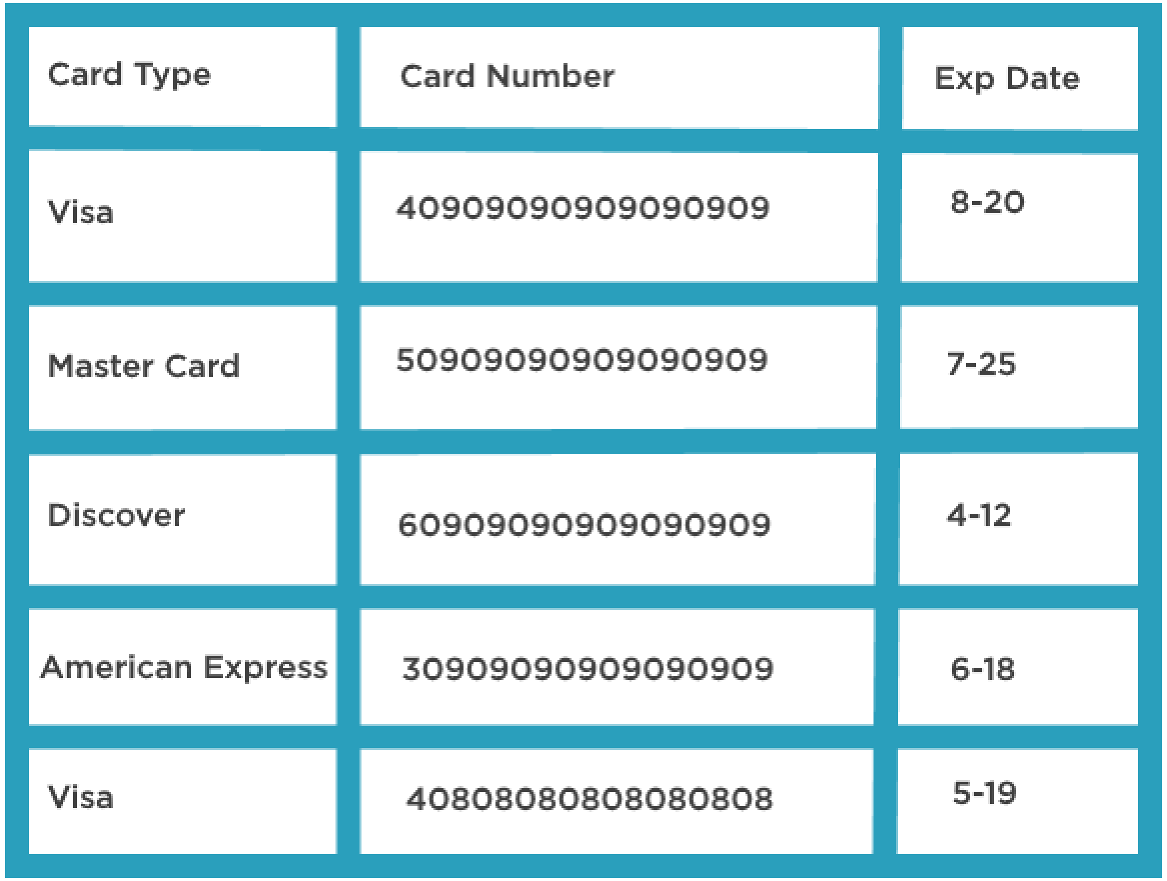
Encrypted data and key physically separate

Security admin and DBA duties separated

Demo

Encrypting our database and managing the database master key

Column Level Encryption



Card Type	Card Number	Exp Date
Visa	4090909090909090909	8-20
Master Card	5090909090909090909	7-25
Discover	6090909090909090909	4-12
American Express	3090909090909090909	6-18
Visa	4080808080808080808	5-19

Column Level Encryption

Card Type	Card Number	Exp Date
Visa	akjpsoifup92ifj0121398ur[la	8-20
Master Card	pkjpofqm2mokmom0(()jo	7-25
Discover	()*9hf29879*9ij2-30nmoksl	4-12
American Express	opfe8ufy9=0()[lk102pm32	6-18
Visa	@*90wnfwkmn0)*pkenfwe	5-19

Encrypted on disk and in all other areas of storage until decrypted by key

Transparent Database Encryption

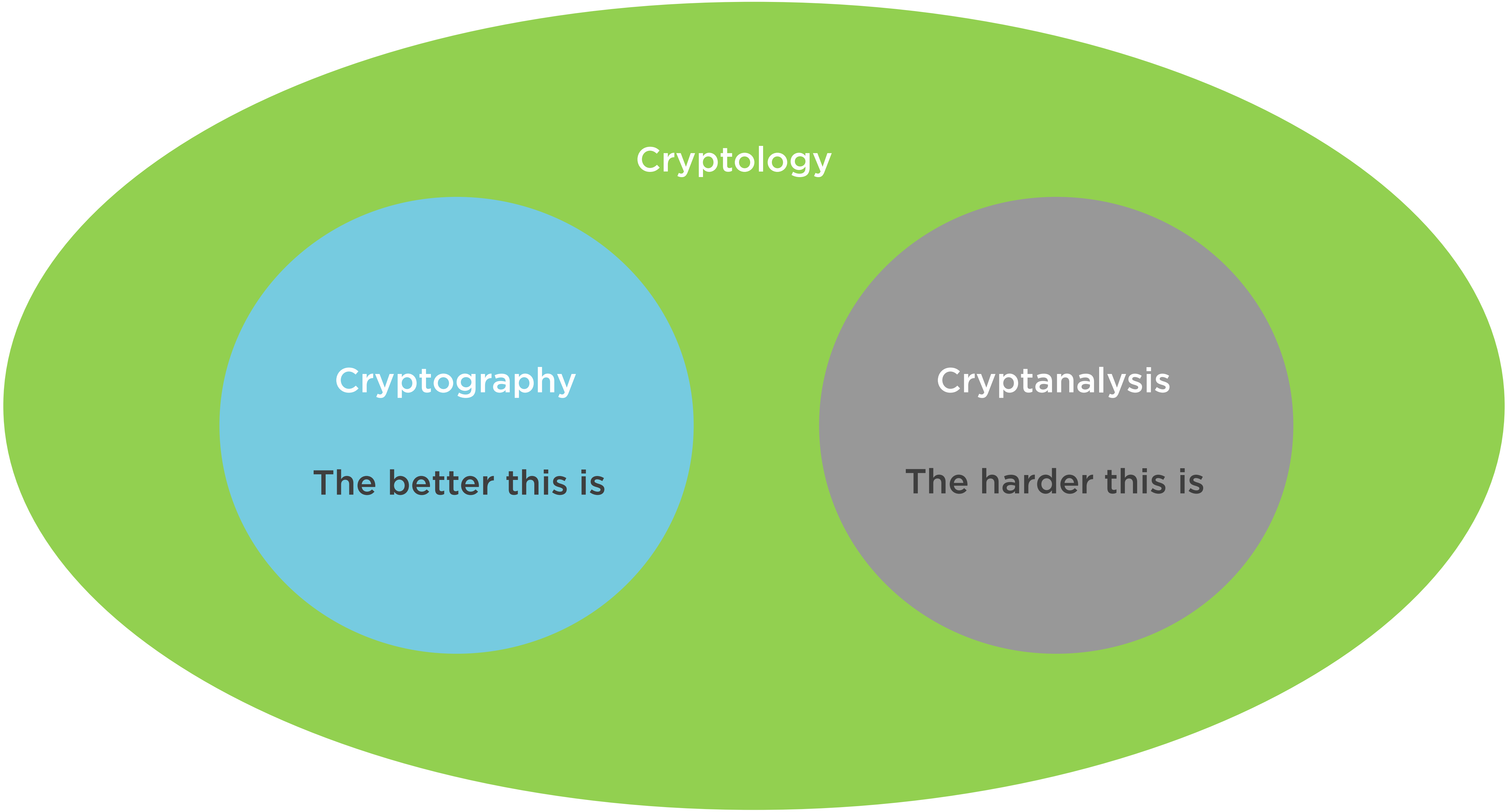
Demo

Create a database encryption key

Create a certificate to protect key

Establish TDE

Manage certificate and other keys



Cryptology

Cryptography

The better this is

Cryptanalysis

The harder this is

SQL Server

- Column Level Encryption
- Database Level Encryption
- Encryption Hierarchy
  - http://bit.ly/2bP8qJD
- Backup Encryption

Encrypting SQL Server Backups

```
BACKUP DATABASE [<your database>]
TO DISK = N‘<your location>'
WITH COMPRESSION,
   ENCRYPTION ( ALGORITHM = AES_256,
   SERVER CERTIFICATE = <certificate you’ve created> )
GO
-- same rules for creating TDE cert apply to backup cert
```

Any compliance or regulatory control that has rules for sensitive data will require some form of encryption

Up Next

Protecting data in transit