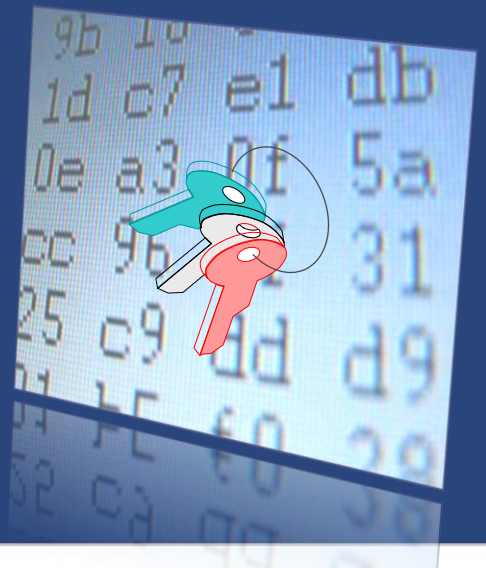
Practical IT security: from encryption algorithms to market products



Luca Mairani

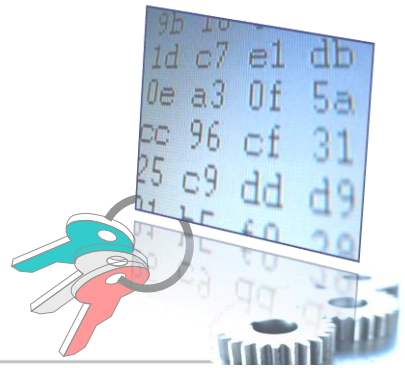
Sales Engineer

SOPHOS ITALIA

luca.mairani@sophos.it

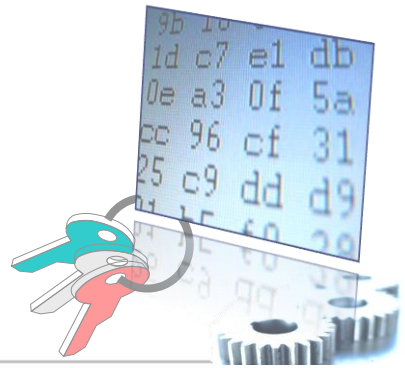
Agenda

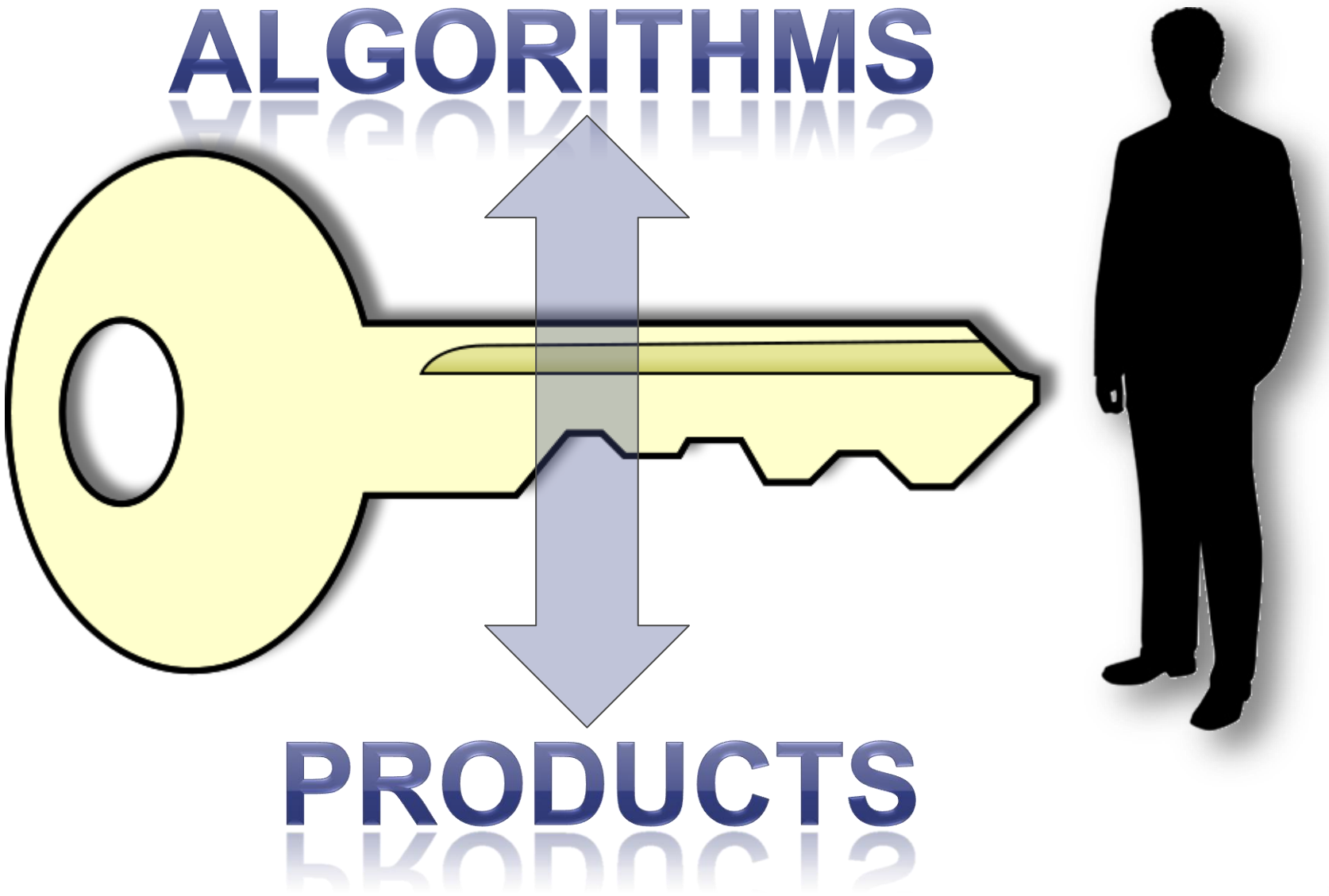
- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



Agenda

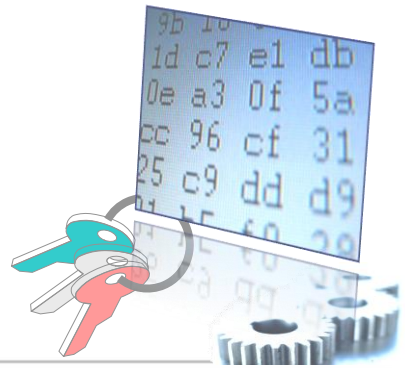
- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt




ALGORITHMS
PRODUCTS

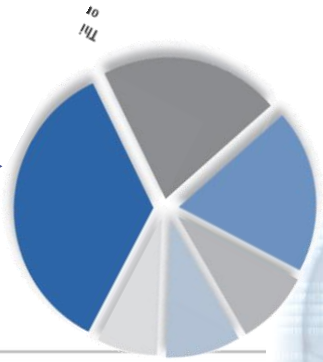
Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



Market pains today

- 4 out of 5 companies have lost confidential data when a laptop was lost Ponemon Institute LLC and Symantec end-user survey, August 2009
- 10% of all notebooks get stolen/lost annually
  Web & Collaboration Strategies 2008
- 1 in 2 USB drives contains confidential information
  Forrester Research, Inc. and Symantec Corp. survey, February 2008.
- 70% of all company data are stored redundant on Endpoints (notebooks, USB sticks) not only on servers
  Ponemon Institute, U.S. Survey: Confidential Data at Risk, August 2008
- Data breaches: increase of 47% over year 2007 – 2008
  Breach List and Statistics - Identity Theft Resource Center (ITCP) Date: 01/12/09
- Top – reason for data breaches in Enterprises:
  Lost laptop other other device – 35%
  Ponemon Institute, 2009, Annual Study: Costs of Security Breaches



Market pains today

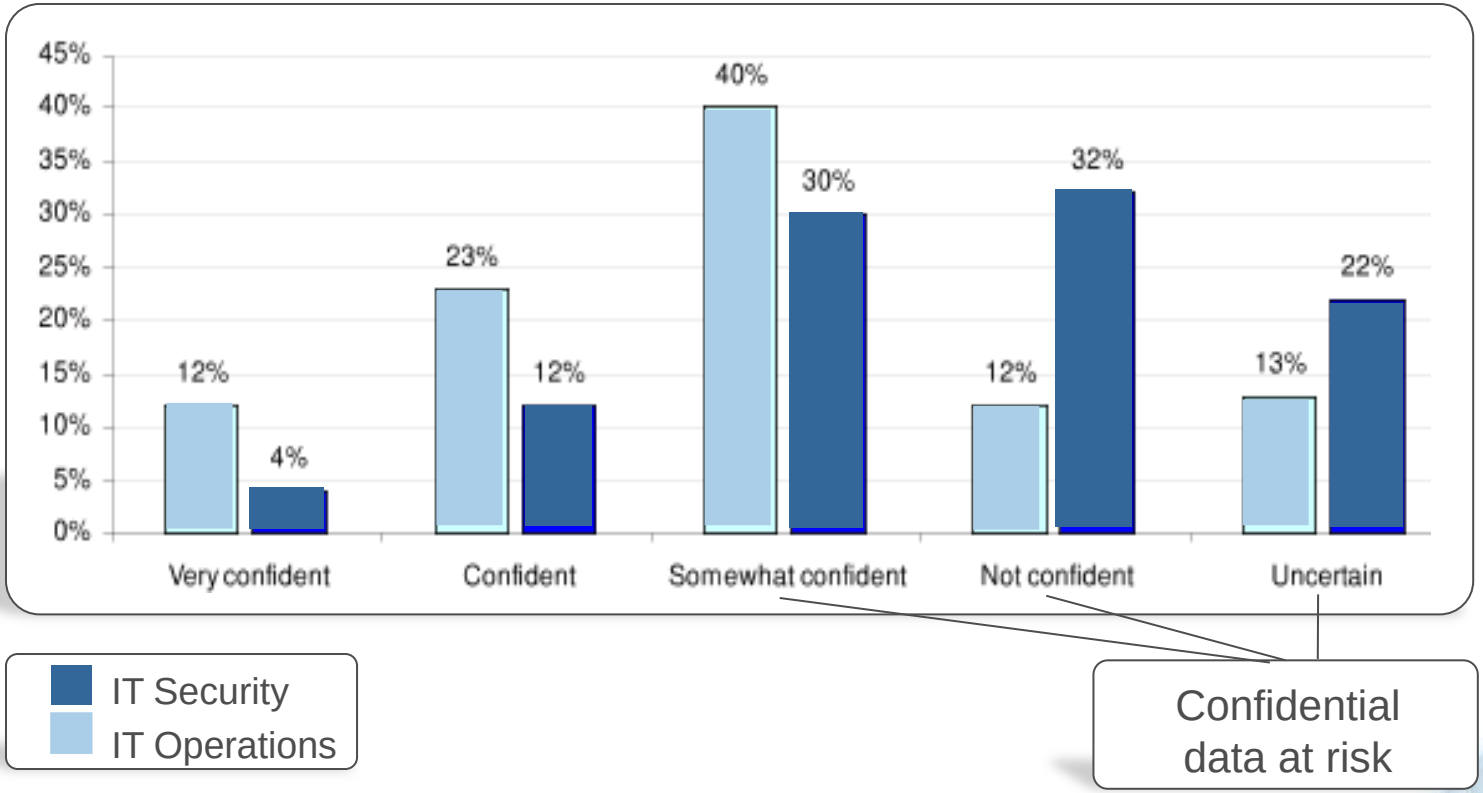
- **12.000** laptops lost or stolen weekly in US airports*

Worldwide
7 million laptops stolen/lost in 2008
Computer Security Institute,2008

**July 2008, www.vnunet.com/vnunet/news/2223012/eu-travellers-losing-laptops-airports*

Market pains today

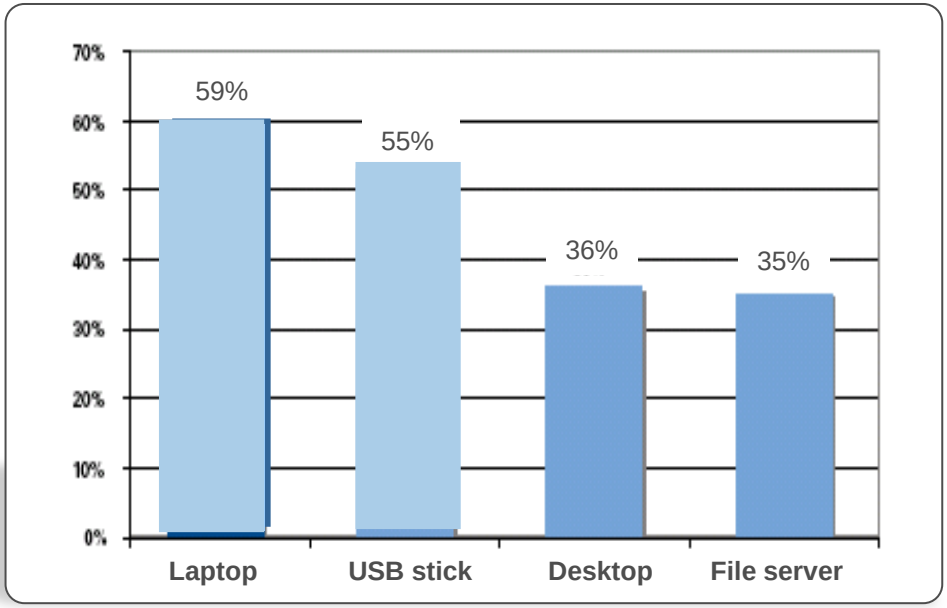
- How confident are you that your current security policies are able to prevent sensitive data from being lost or stolen?



Ponemon Institute: 2009 Security Mega Trends
http://viewer.bitpipe.com/viewer/viewDocument.do?accessId=9078616

Market pains today

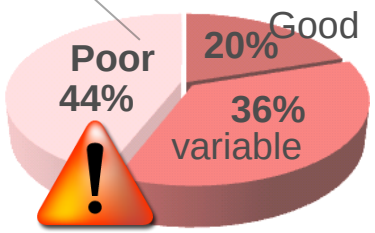
- What is the probability that devices contain unprotected confidential data?



Confidential data at risk

How would you rate your employees´ attitude towards mobile security?

Freedom Dynamics, Feb. 2007, Secure Mobile Working



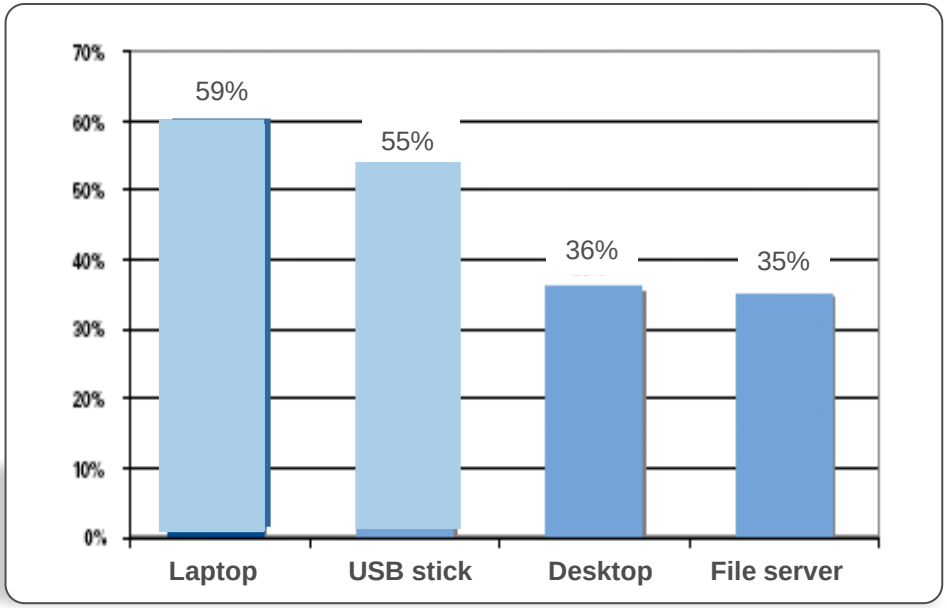
70% of all company data is stored redundant on endpoints (laptop, desktop, USB stick)

Ponemon Institute: Confidential Data at Risk, 2007

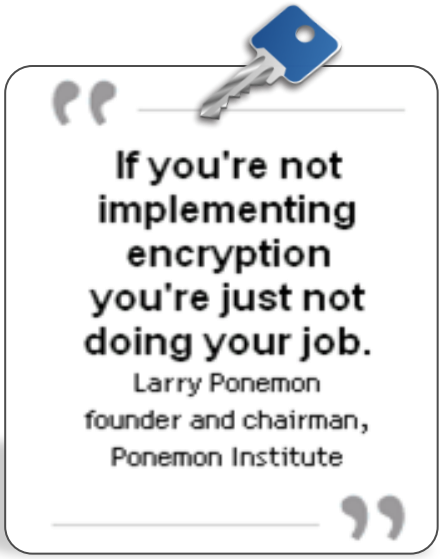
Ponemon Institute
U.S. Survey: Confidential Data at Risk, August 2007

Market pains today

- What is the probability that devices contain unprotected confidential data?



Confidential data at risk

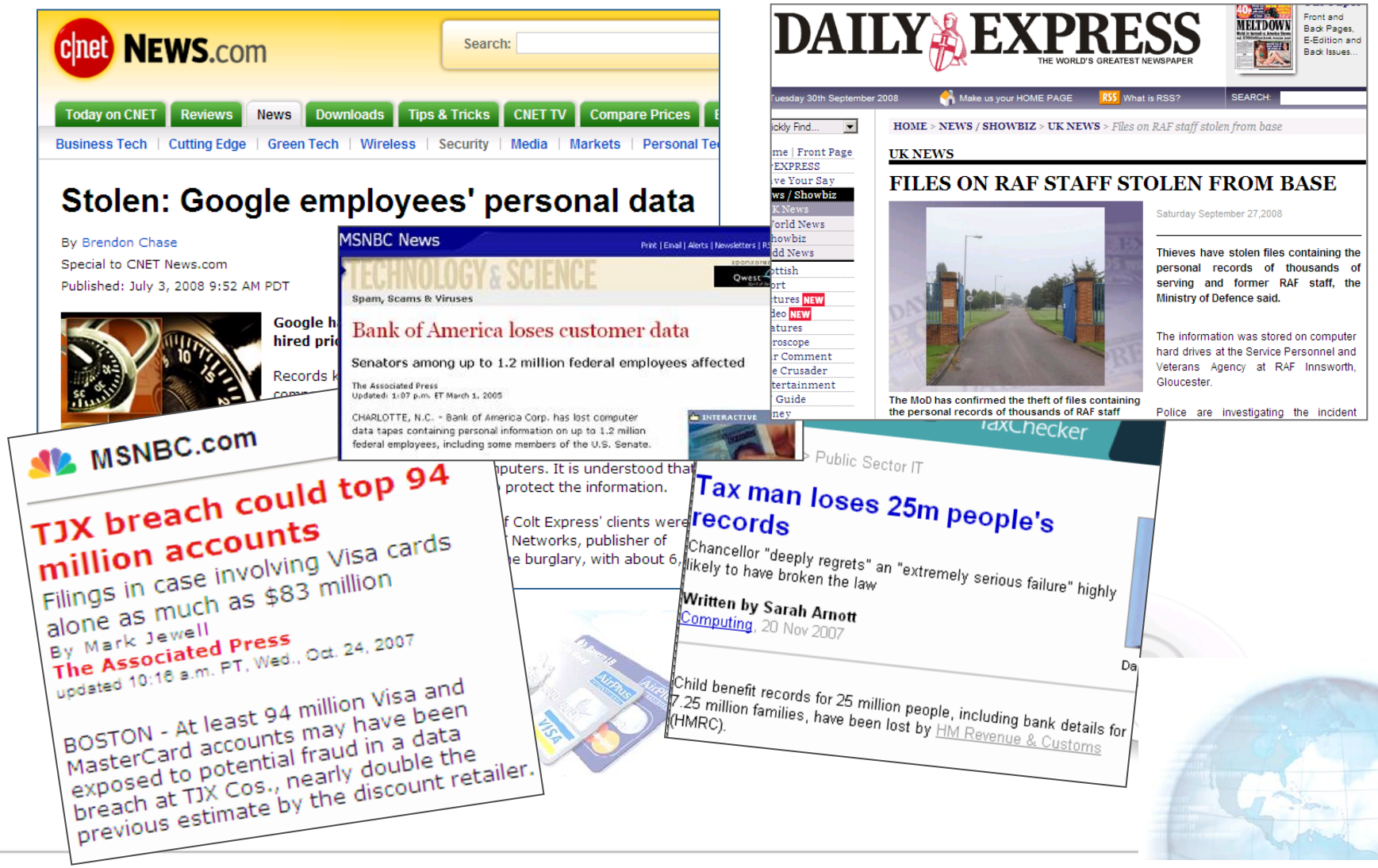


70% of all company data is stored redundant on endpoints (laptop, desktop, USB stick)

Ponemon Institute: Confidential Data at Risk, 2007

Ponemon Institute
U.S. Survey: Confidential Data at Risk, August 2007

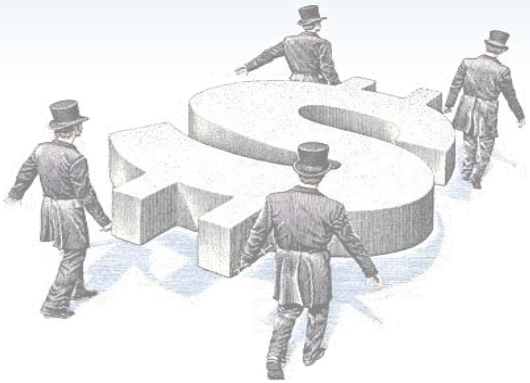
Headlines to be avoided



Business impact of data breaches

'Enterprise data loss' cost businesses nearly $105 billion last year

according to U.S. government, 2009

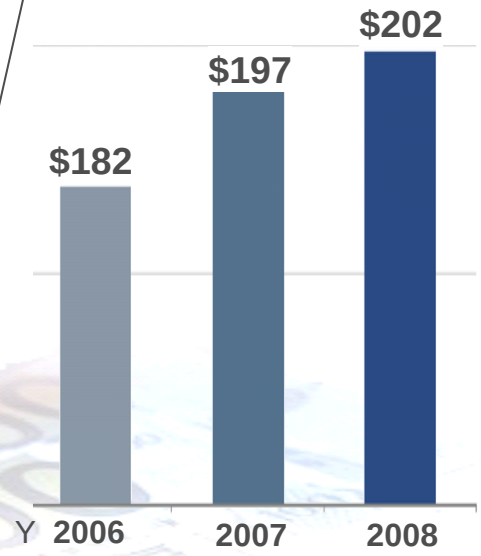


http://searchsecurity.bitpipe.com/detail/RES/1233787228_895.html?li=169330&src=KA_RES_20090226&asrc=EM_KAR_5956107&uid=5097956

Business impact of data breaches

Incident	Date	Victims	Potential Cost
Leak of US military personnel and veterans' data	May 2006	28.7 million	$45 billion
Laptop stolen from Nationwide Building Society, UK	Aug 2006	11 million	$1.5 billion
A portable hard drive with company data stolen by insider at Dai Nippon Printing	Jul 2006	8.64 million	$1.2 billion
A laptop stolen from the US war veterans' medical centre in Birmingham with doctors' and patients' personal data	Jan 2007	1.8 million	$367 million
A mobile computer stolen from Computer Services (ACS) with personal client data	Oct 2006	1.4 million	$320 million
Laptop lost by subcontractor for Texas Guaranteed with TG's client data	May 2006	1.3 million	$237 million
Laptop stolen from a Boeing employee's car	Nov 2006	382,000	$147 million
Laptop stolen from CS Stars with names, addresses and Social Security numbers of New York workers	Jul 2006	540,000	$84 million
Laptop with personal data stolen from an employee of the accountancy firm Hancock Askew	Oct 2006	401,000	$73 million
Investigation at the Vassar Brothers medical centre found the loss of a laptop and backup disk with patient data	Jan 2007	257,800	$47 million

Top 10 Mobile Devices Leaks (2006 -2007)



Average per record cost of a data breach

Ponemon Institute:
2008 Annual Study: Cost of a Data Breach

INFOWATCH http://www.infowatch.com/threats?chapter=162971949&id=207784708

Business impact of data breaches

- HSBC has been fined **£3.2million** for losing personal details of more than 180,000 customers (unencrypted CD)
- HSBC co-operated with the FSA investigation and received a 30% discount from the potential maximum fine of £4.55 million.

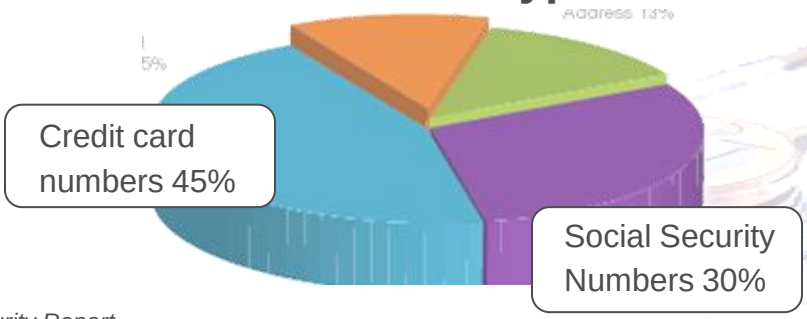
FSA = Financial Services Authority

Financial News, Wednesday, July 22, 2009

Business impact of data breaches

- Data breach at a leading credit card processor (January 2009)
  - Company processes cards for app. 250,000 businesses in US
  - Result: **Spending < US$10 million in …**
    - Legal fees/bills
    - Fines from MasterCard and Visa
    - Administrative costs
  - Company reported a quarterly loss of < US$2 million.

Lost record types



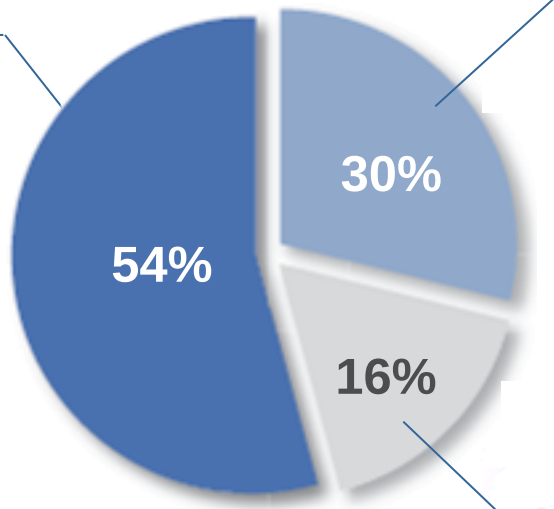
Source: Cisco 2009 Midyear Security Report

Business impact of data breaches

- Average cost per compromised record: for financial firms **$197 – $239**

Customer Costs

- Brand damage
- Loss of existing customers
- Recruiting new customers



Incremental Costs

- Legal fees
- Audit & accounting fees
- Notification of customers
- Free or discounted service to customers
- Call center expenses
- Public & investor relations
- Internal investigations

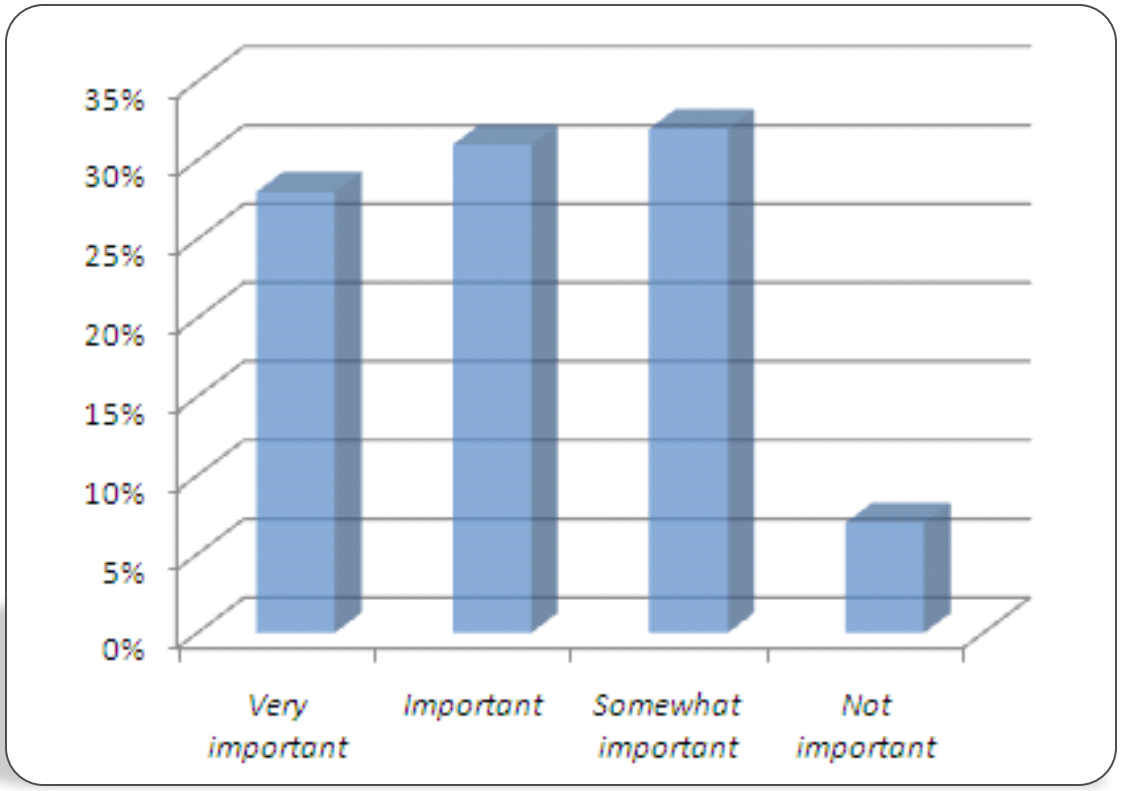
Productivity Costs

- Lost employee productivity

Source: Ponemon Institute, Nov. 2008
www.ponemon.org/press/06-25-07-Ponemon_Consumer_Survey_FINAL.pdf

Data Protection

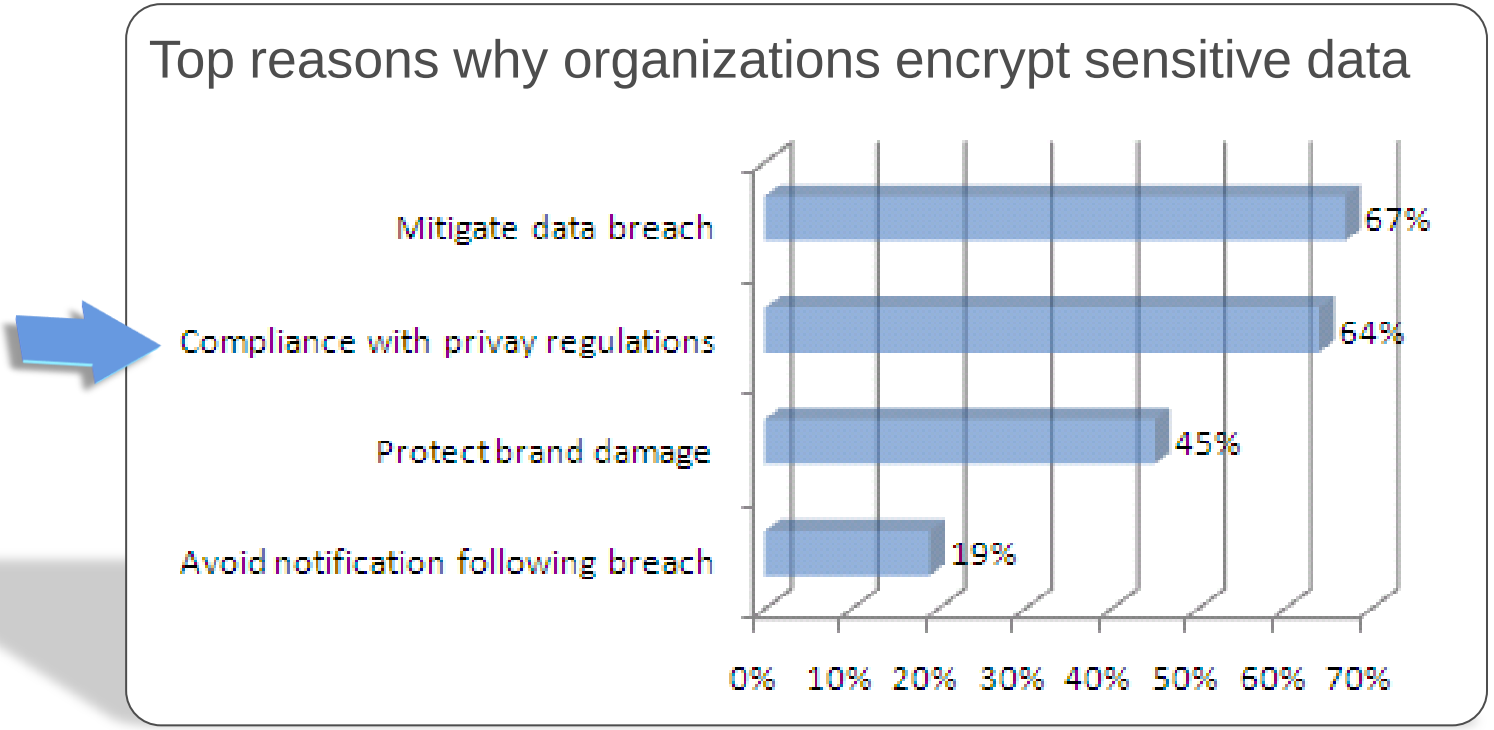
- Organizations recognize importance of data on mobile devices
  - More than half the respondents considered the data to be either important or very important



Ponemon Institute, LLC
2009 Annual Study: U.S. Enterprises Encryption Trends

Data Protection & Compliance

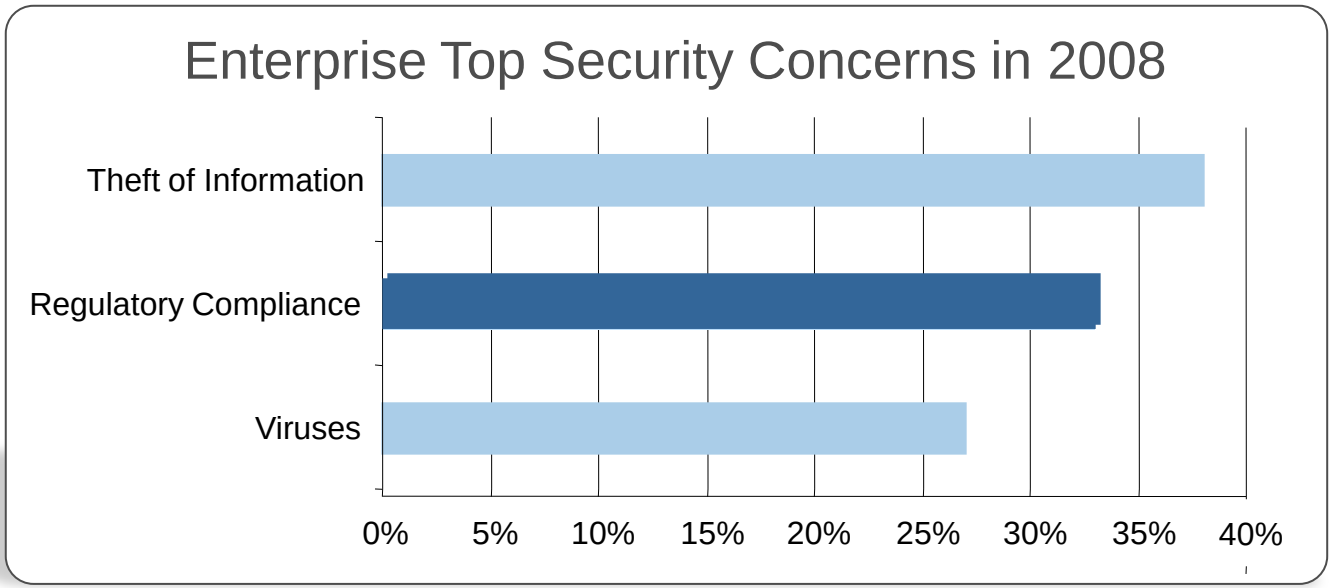
- Compliance drives companies to focus on encrypting their data
  Aberdeen Group, May 2008



Ponemon Institute, LLC
2009 Annual Study: U.S. Enterprises Encryption Trends

Data Protection & Compliance

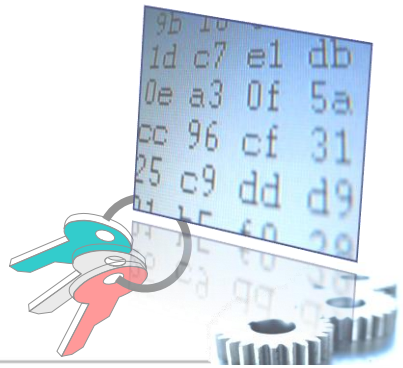
- Data theft and regulatory compliance replaces malware as top security concern



Cisco Security Survey 2008
http://www.channelregister.co.uk/2007/04/19/security_fears_poll/

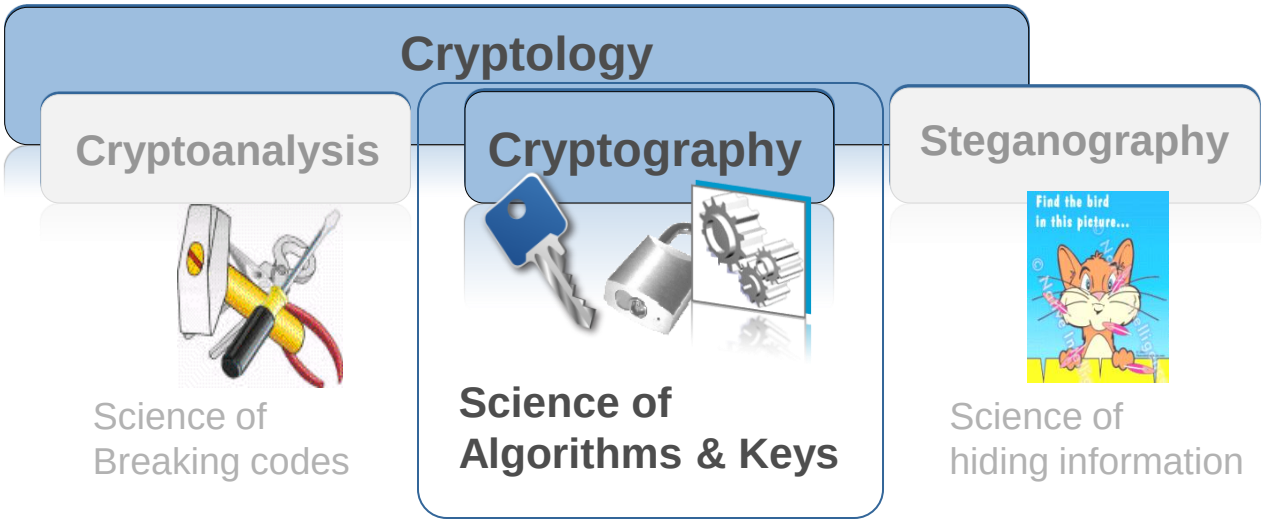
Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



Cryptology

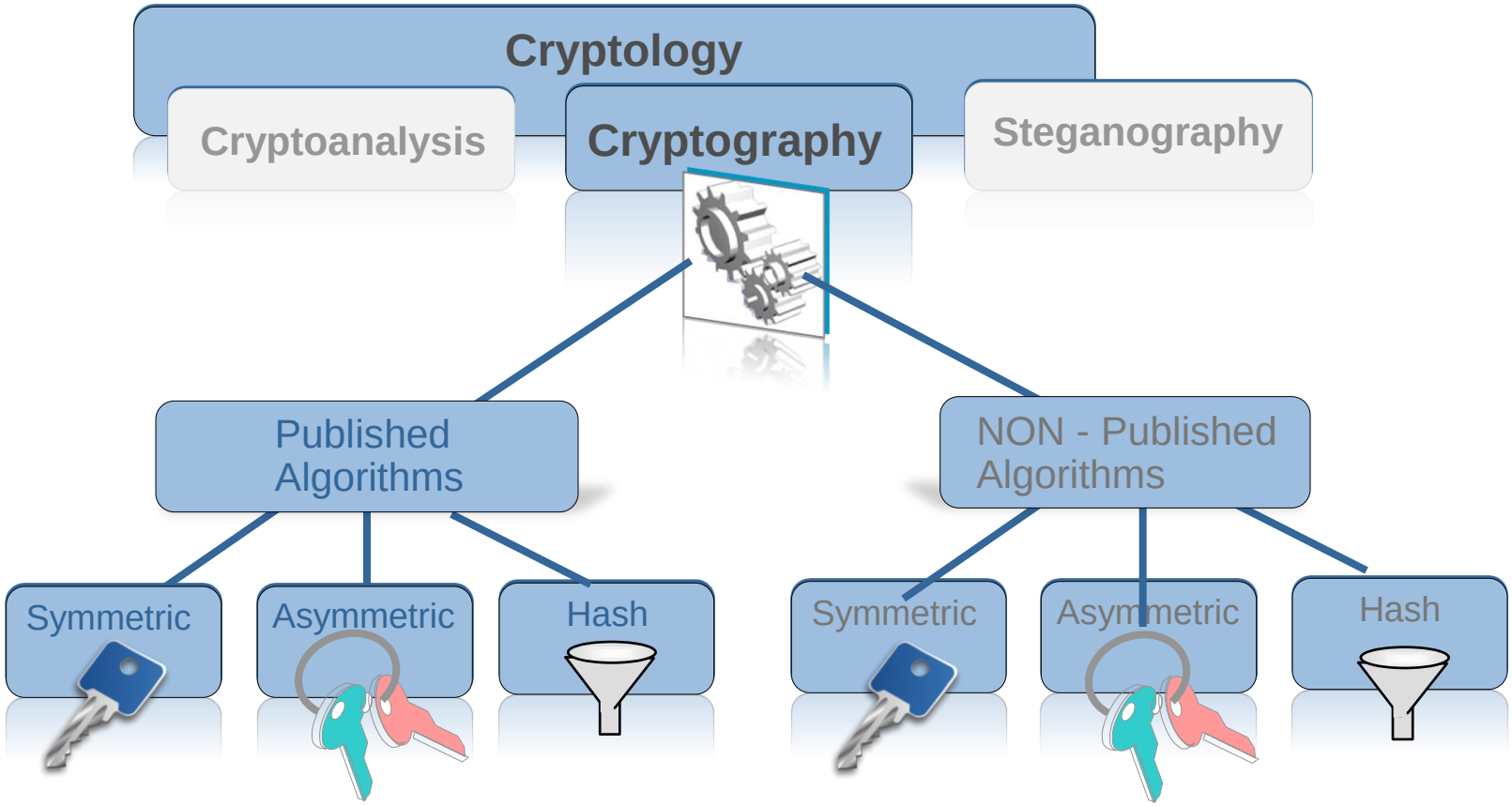
Positioning in general



- Cryptography …
  - allows us to take existing business from the face-to-face world into the world of computers and networks.
  - Can transform the Internet from a toy to a serious business tool
  - is an essential part of today's information systems

Cryptography and its Subclasses

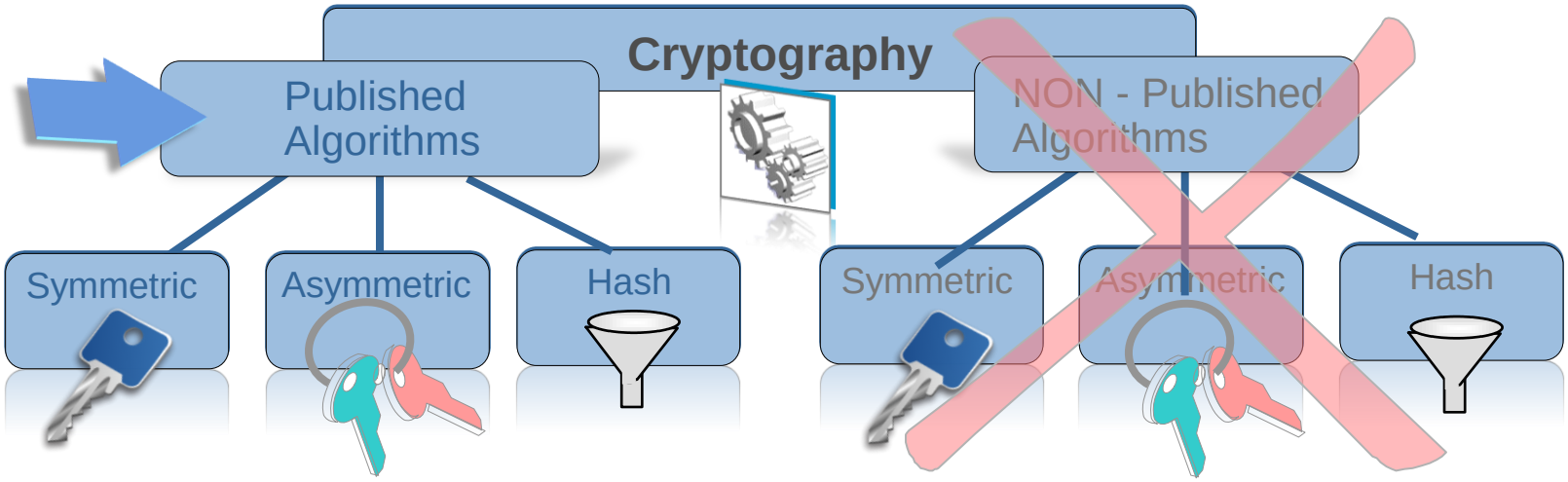
Definition



Cryptosystem

Published – Non published Algorithms

- Almost all unpublished (non-published) algorithms are insecure
- NEVER trust a non - published (proprietary or secret) algorithm
- Also many published algorithms are insecure
  - BUT: ***Because source code is open (published) the strength of its implementation can be checked by specialists***

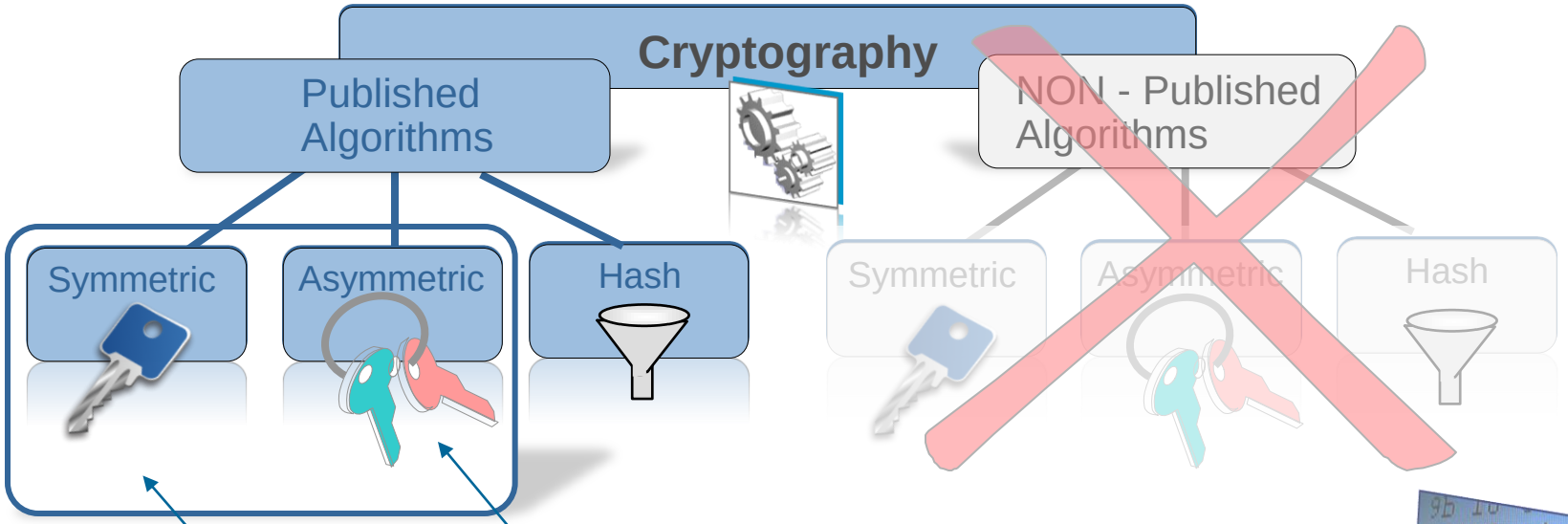


Remark: Inside Sophos we are only using published algorithms

Cryptosystem

Basics/Terminology

- Modification of plain text into an unreadable set of characters using Algorithms and Keys



Well known Symmetric

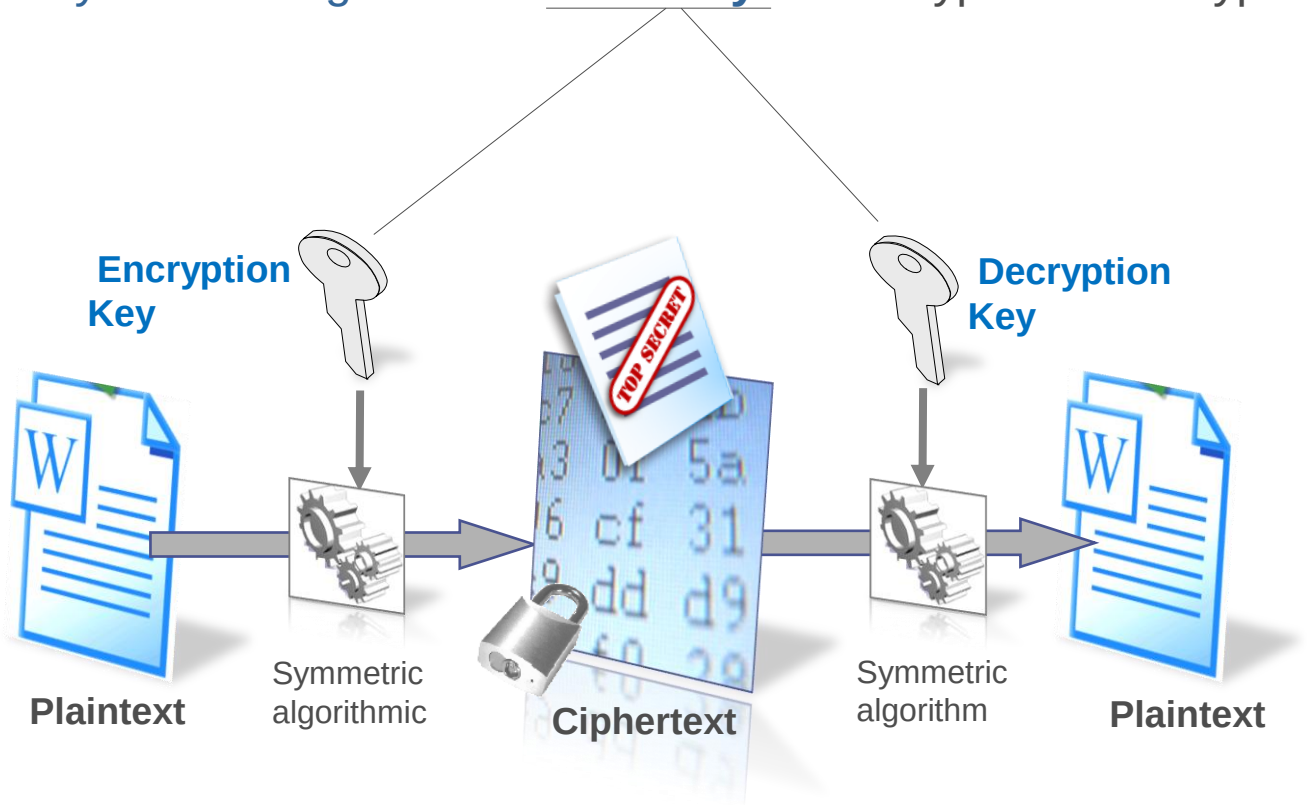
- **DES**
- **IDEA**
- **AES** (Rijndael)

Well known Asymmetric

- **RSA**

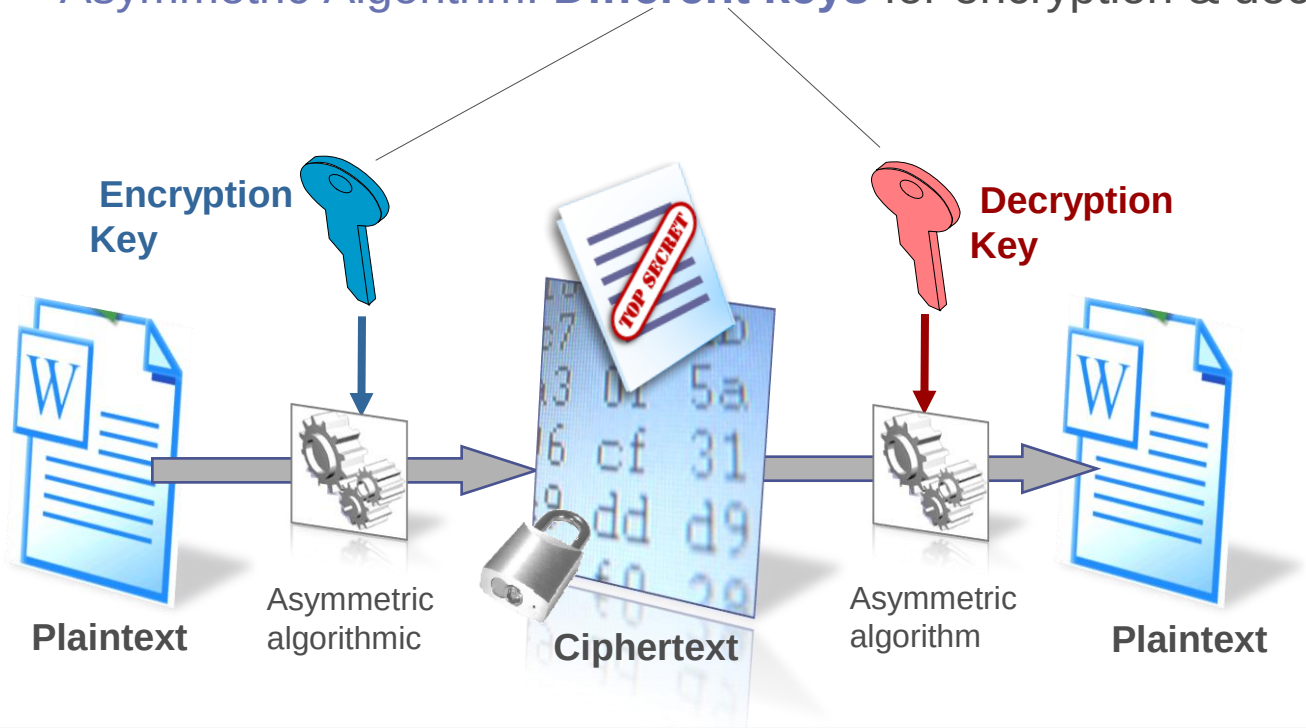
Cryptography
In general

- Encryption and decryption generally require the use of some secret information, referred to as a key
  - Symmetric Algorithms: **Same key** for encryption & decryption



Cryptography
In general

- Encryption and decryption generally require the use of some secret information, referred to as a key
  - Symmetric Algorithms: **Same key** for encryption & decryption
  - Asymmetric Algorithm: **Different keys** for encryption & decryption

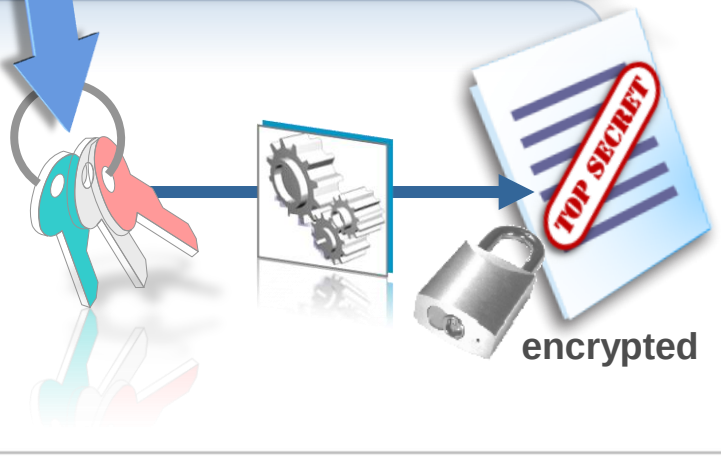


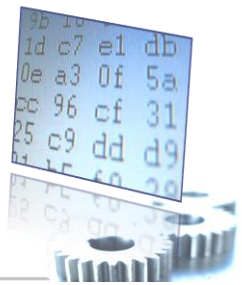
Cryptosystems

Fundamental Principle: Published Algorithm

The security of a crypto system depends NOT on the secrecy of the algorithm itself

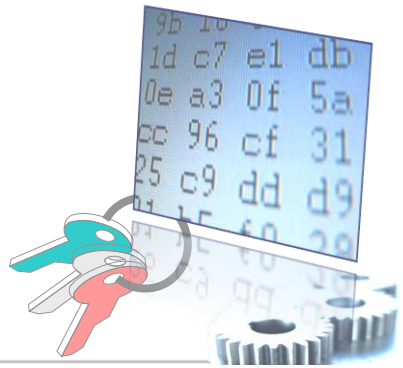
The security depends ONLY on the secrecy of the used key





Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



Symmetric Algorithms

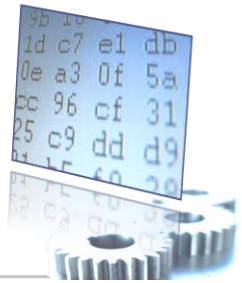
Secure Key Length

- Key length must be large enough to be protected against trying out all possible key combinations (permutations)

Possible keys (permutations)

- 32 Bit key length → 2^{32} = ***4.300.000.000***
- 40 Bit key length → 2^{40} = ***1.100.000.000.000***
- 56 Bit key length → 2^{56} = ***72.000.000.000.000.000***
- 128 Bit key length → 2^{128} =
  340.000.000.000.000.000.000.000.000.000.000.000.000

- IDEA
- Blowfish
- AES



PGP, Whitepaper: Introduction to Cryptography

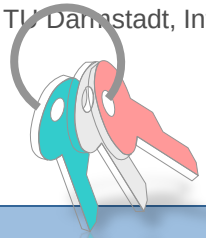
Symmetric Algorithms

Secure Key Length

- Key length must be large enough to be protected against trying out all possible key combinations (permutations)

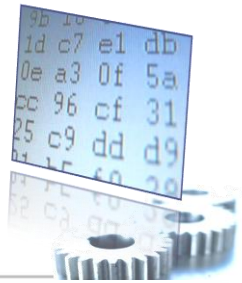
Investment to crack (US $)	64 bit	80 bit	128 bit
1 Mio	37 days	7.000 years	10^{18} years
10 Mio	4 days	700 years	10^{17} years
100 Mio	9 h	70 years	10^{16} years
1 Billion	1 h	7 years	10^{15} years
10 Billions	5,4 min.	245 days	10^{14} years
100 Billions	32 sec.	24 days	10^{13} years

Sicherheit bei Finanztransaktionen übers Internet - TU Darmstadt, Informatik 2007



Brute Force Attack: Time to find the key

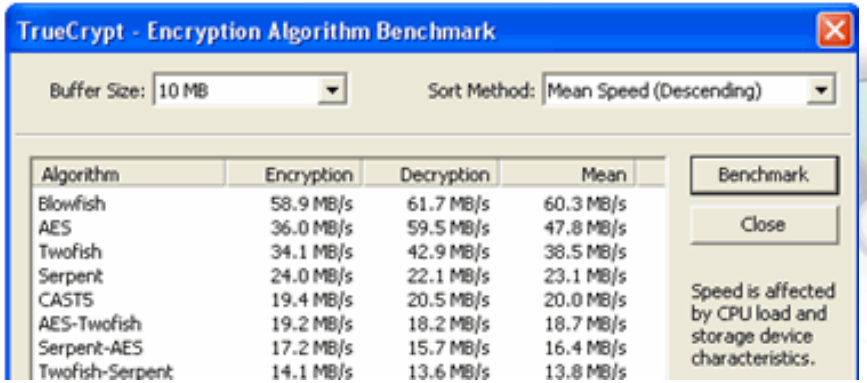
Remark: The Universe exits since 10^{10} years



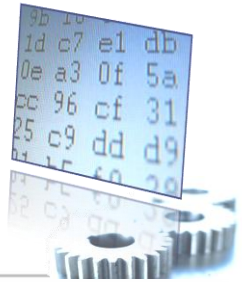
Symmetric Algorithms

Advantage

- Speed/Performance
  - Rule of the thumb: 1000 times faster than asymmetric algorithms
  - Example: AES Encryption
    - 60 MB/sec on standard PC
    - CD content secure encrypted in approx. 10 seconds



  - Attention: Password lost → Data lost

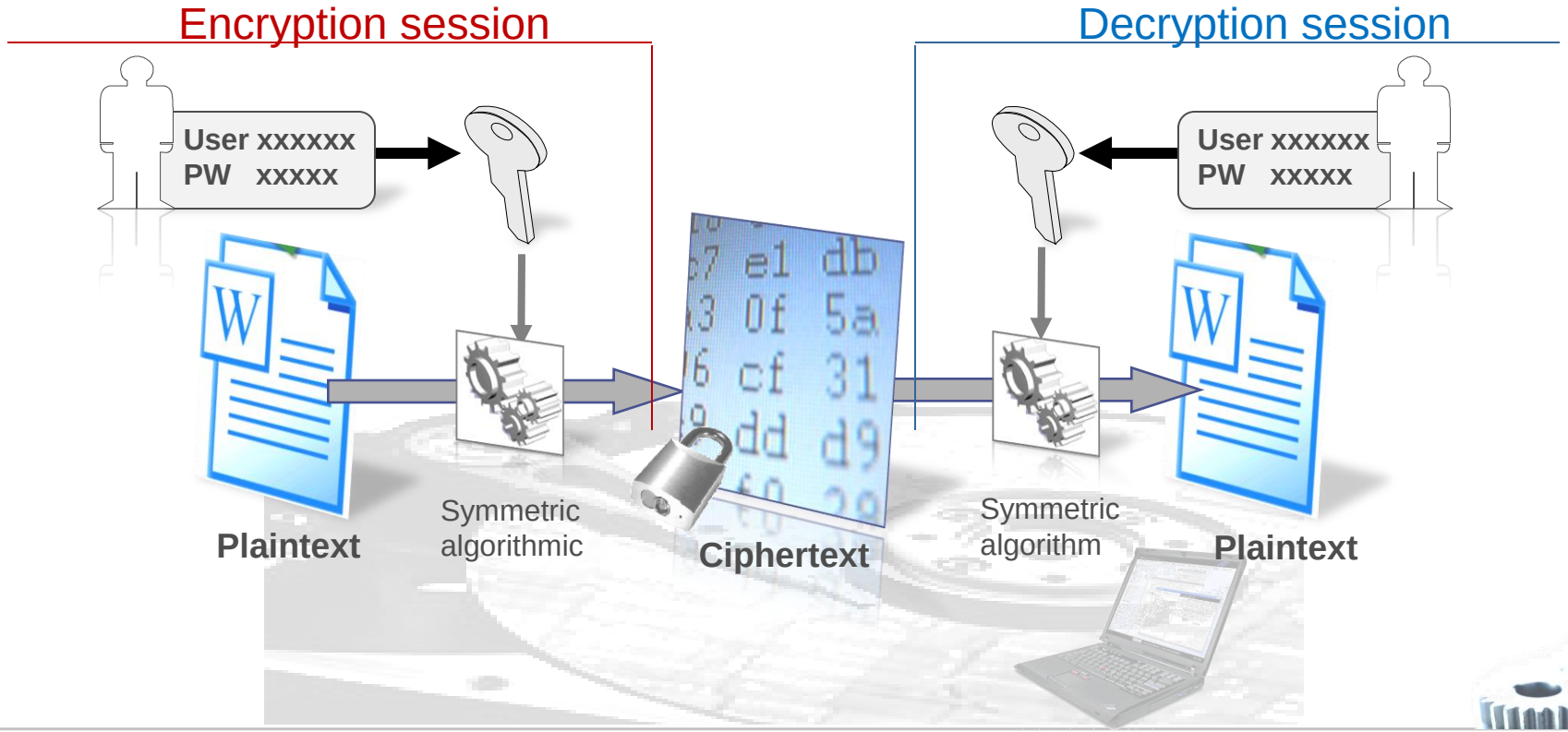


http://blog.davebouwman.net/content/binary/tc2.gif

Use of Symmetric Algorithms

In Theory

- Principle #1
  - For encryption & decryption = Same key = Same Password
  - Key/Password must be kept secret

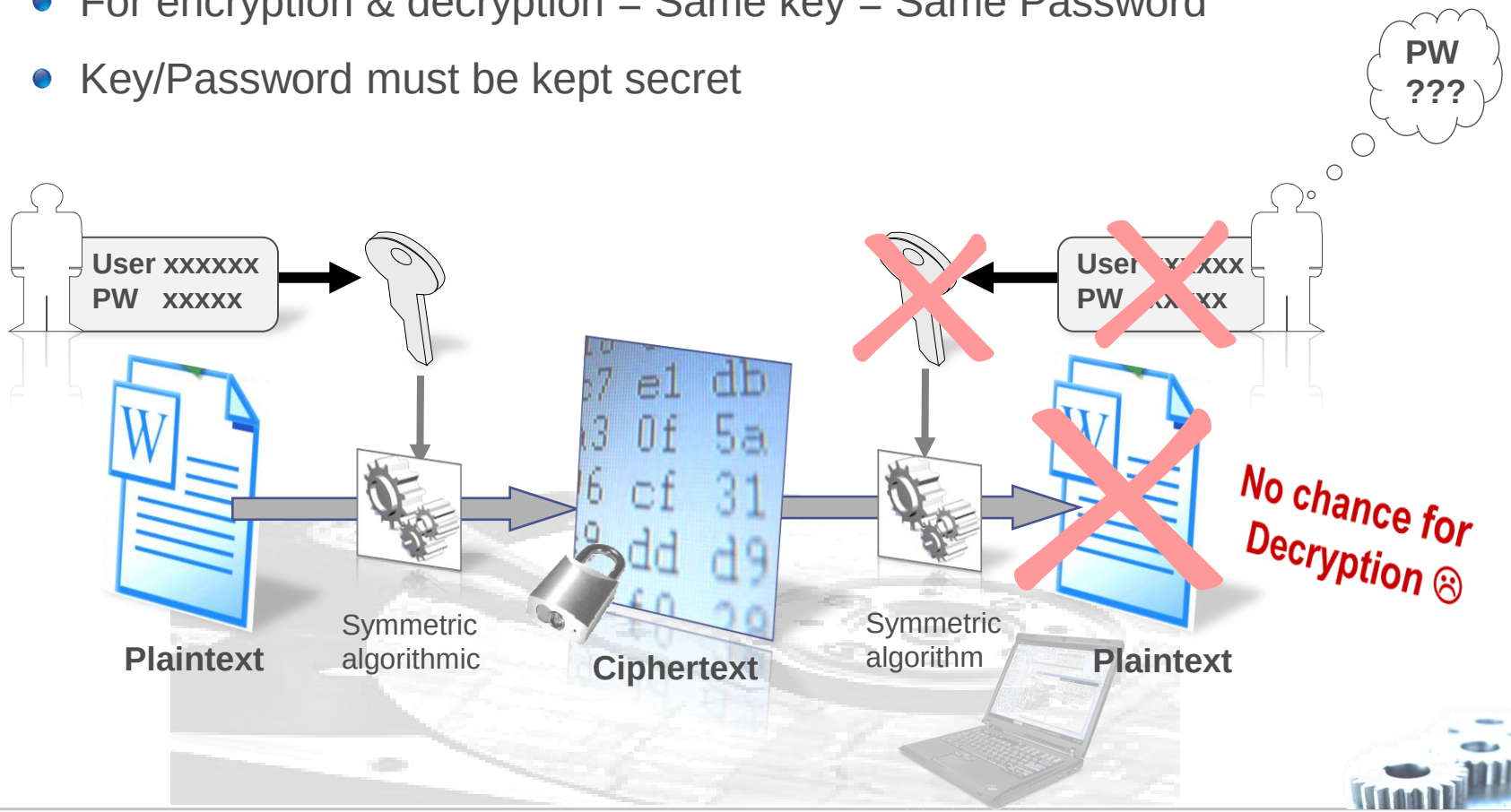


Use of Symmetric Algorithms

Challenge: *Password lost …*

Solution to solve this problem later in this session ☺

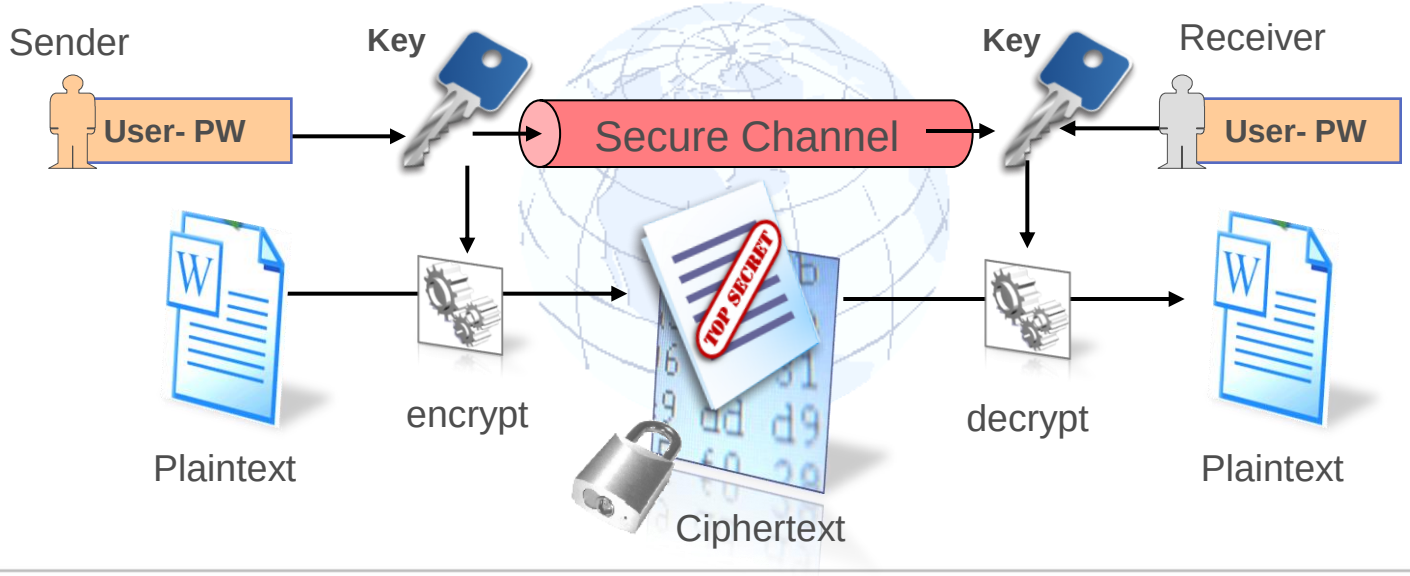
- Principle #1
  - For encryption & decryption = Same key = Same Password
  - Key/Password must be kept secret



Symmetric Algorithms

Disadvantage

- Key Management
  - Symmetric keys will have to be distributed through secure channels (= encrypted channel)
  - Because all keys must remain secret, symmetric cryptosystems has the problem of providing secure key management
    - Especially in systems with a large number of users (workgroups)

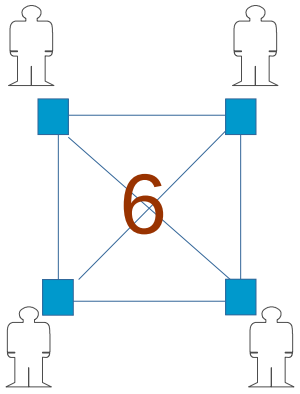


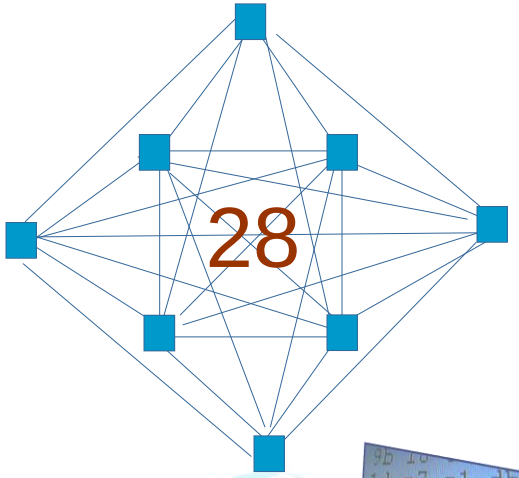
Symmetric Algorithms

Disadvantage

- Key Management
  - Symmetric keys will have to be distributed through secure channels = keys must be encrypted
    - Especially in systems with a large number of users (workgroup)
- Example
  - n-partner need
    - n = 4 → 6 keys
    - n = 6 → 15 keys
    - n = 12 → 66 keys
    - n = 1000 → 499500 keys

n* (n-1)/2 keys

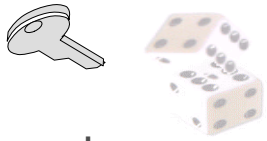




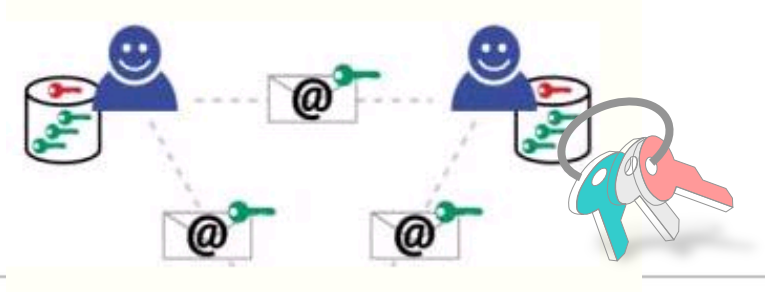
Symmetric Algorithms

Summary- Characteristics

- **Advantages ☺**
  - Good Performance (speed)
    - Rule of the thumb: 1.000 times faster than asymmetric algorithms
    - Perfect to encrypt mass data
  - Easy Key Generation
    - Random generated
    - Derivate from a password

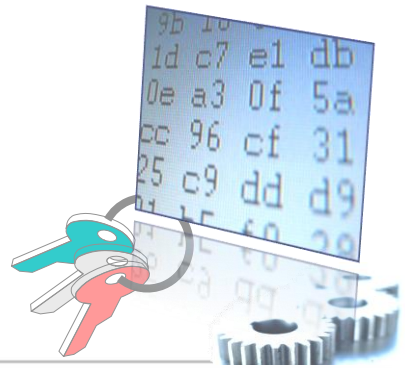


- **Disadvantage ☹**
  - Key Management in big workgroup environment
  - Keys will have to be distributed through secure channels



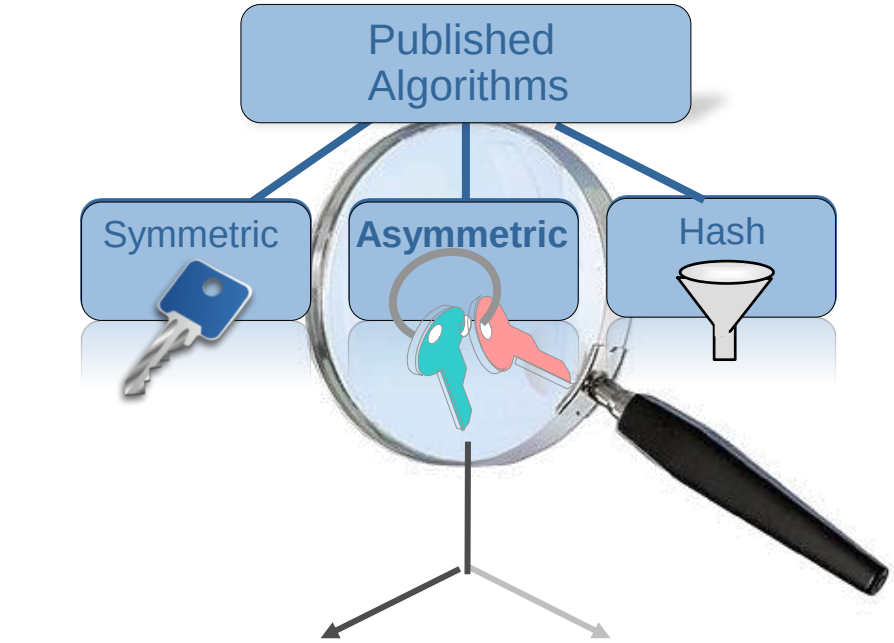
Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



Cryptography

Types of Algorithms → Asymmetric



Factoring

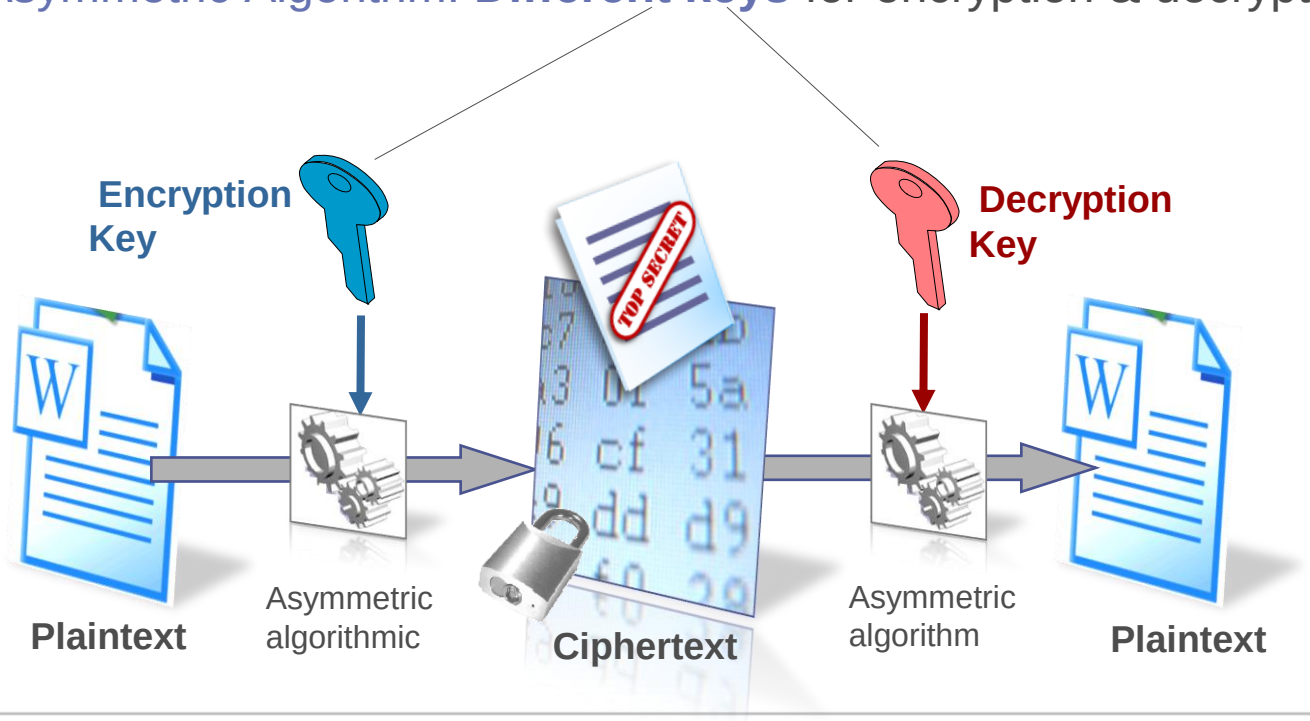
- **RSA**
- ..

Discrete Log.

- Diffie Hellman
- DSA
- Elliptic Curves
- ElGamal

Cryptography
In general

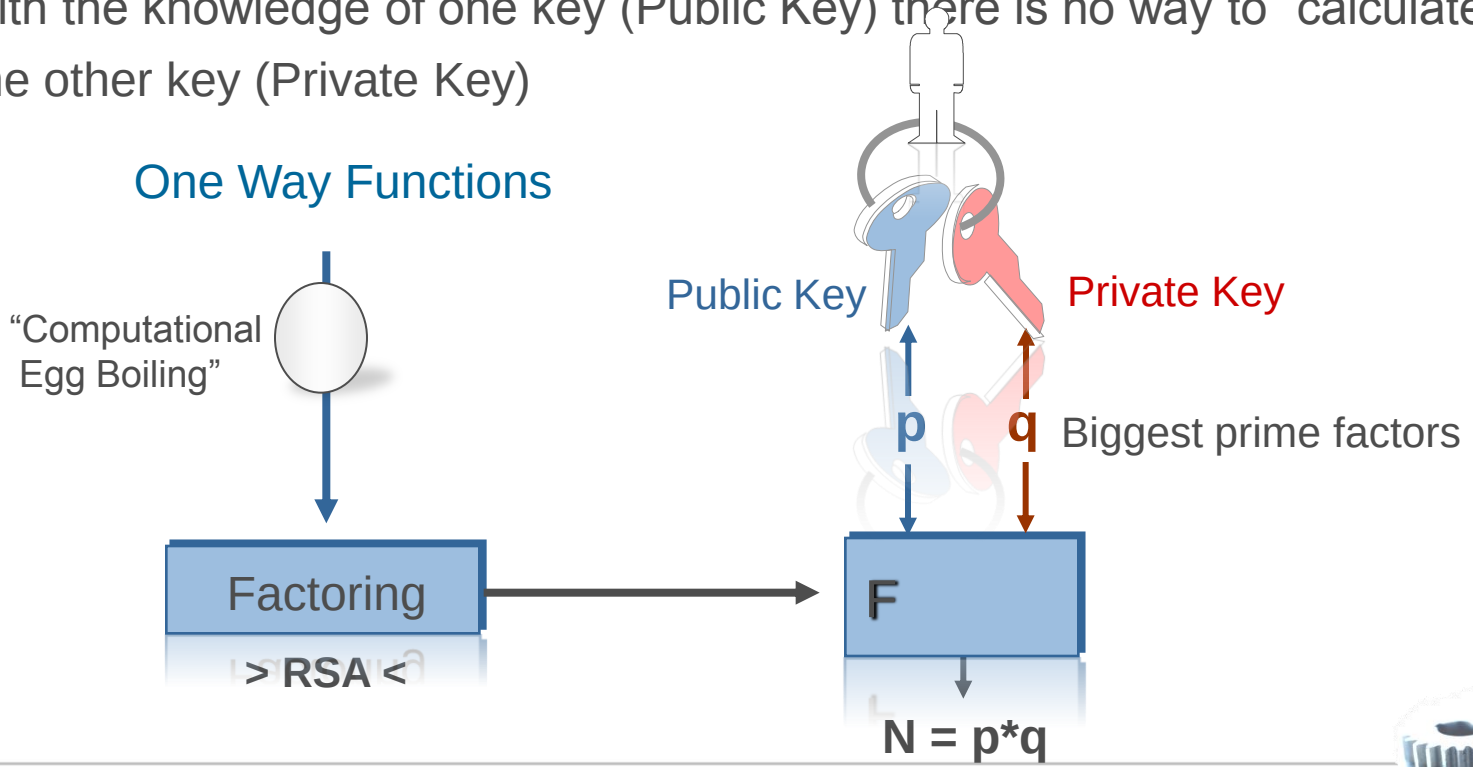
- Encryption and decryption generally require the use of some secret information, referred to as a key
  - Symmetric Algorithms: **Same key** for encryption & decryption
  - Asymmetric Algorithm: **Different keys** for encryption & decryption



Asymmetric Algorithms

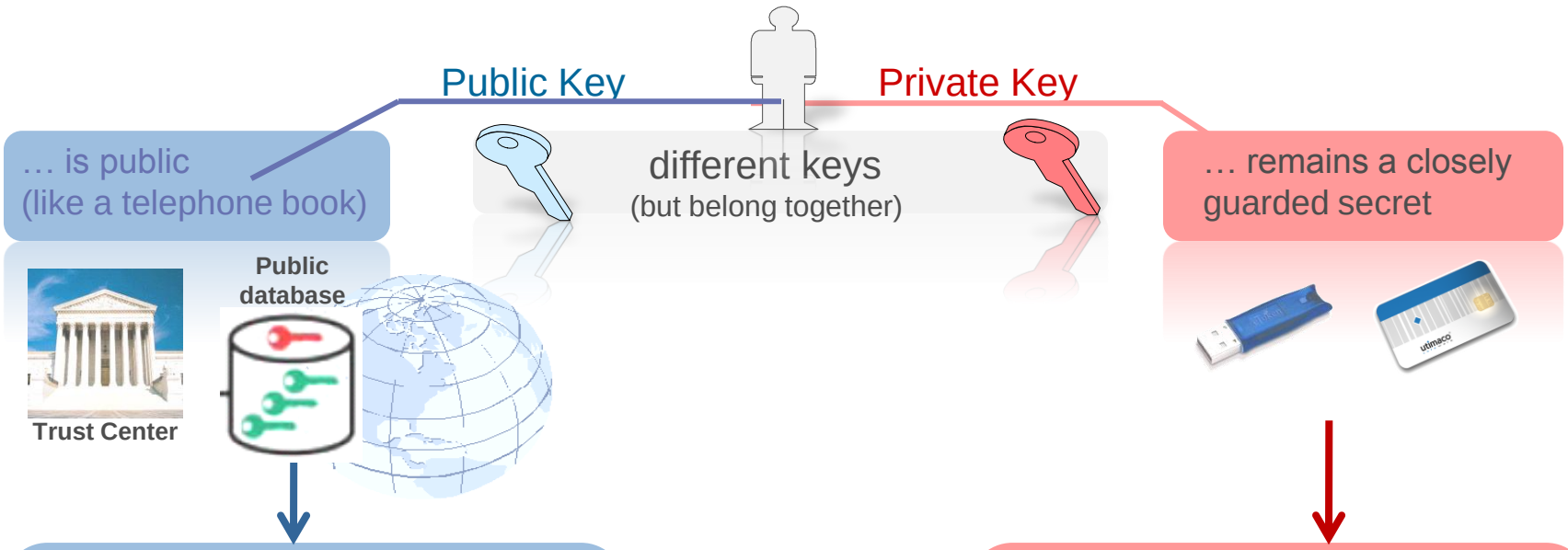
Basics: Key Generation

- Asymmetric cryptography uses two different but mathematically related keys for encryption and decryption
- Key pair belongs together, but …
  - with the knowledge of one key (Public Key) there is no way to “calculate” the other key (Private Key)



Asymmetric Algorithms

Basics: Key Storage



Public Key (PuK)

which can be distributed widely without regard to confidentiality (Public Database, PKI)

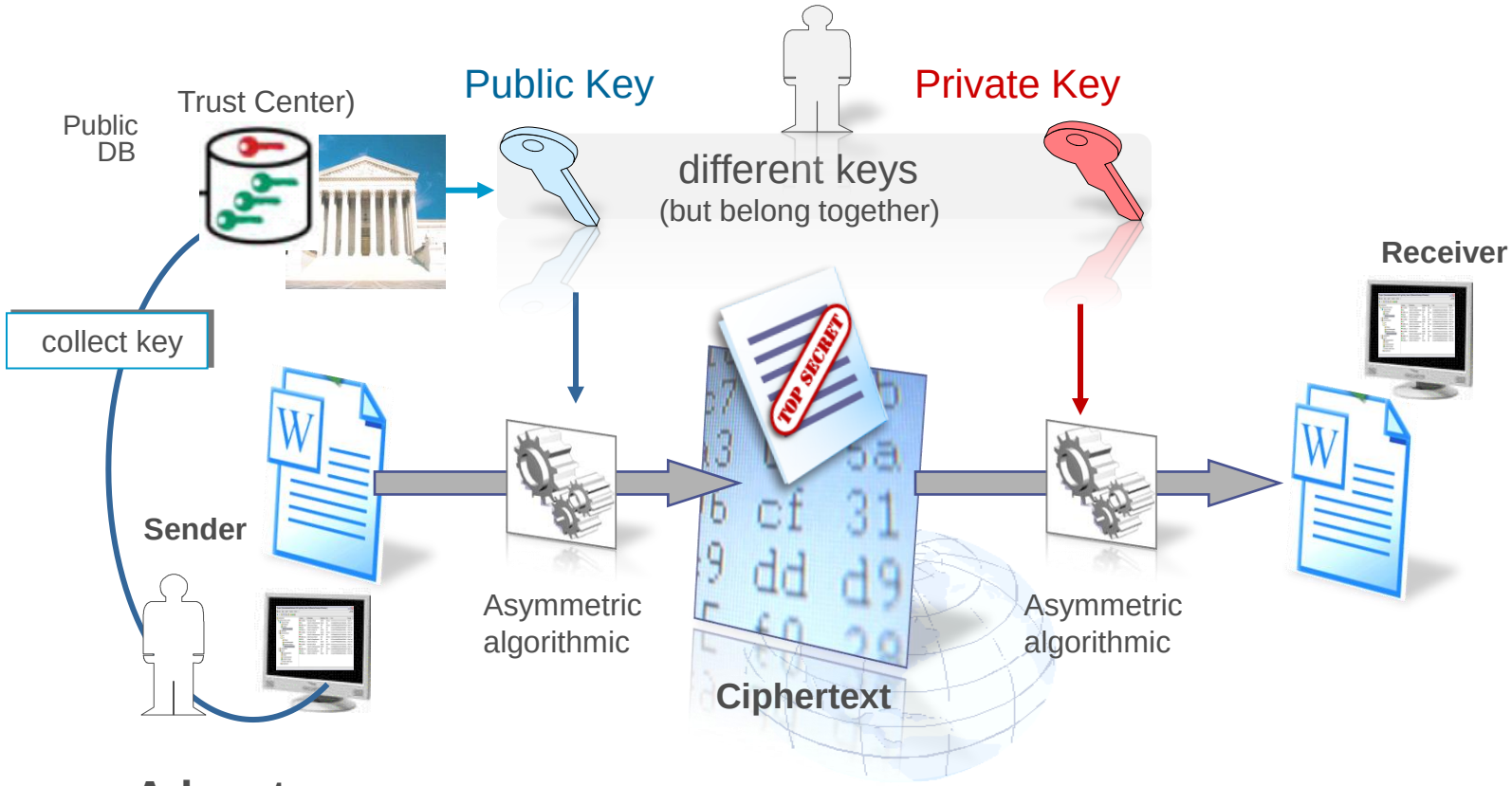
Private Key (PrK)

which must be kept confidential
- on Smartcard, Token, …
- encrypted keyfile (PKCS#12)

PKCS = Public Key Crypto Standard

Asymmetric Algorithms

Encryption for Receiver (Theory)



Advantage:

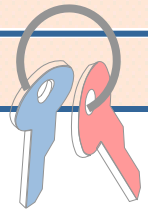
- Only recipient can decrypt (confidentiality)
- No secure key exchange needed because Public key is public

Algorithms

Secure Key Length - Comparison

Symmetric Keys	RSA Keys	Time to crack …
56 Bit	430 Bit	5 minutes
80 Bit	760 Bit	600 months = 50 years
98 Bit	1020 Bit	3 mio years = $3X10^6$ years
128 Bit	1620 Bit	10^{16} years

Source: RSA Labs, Network World, June 2006

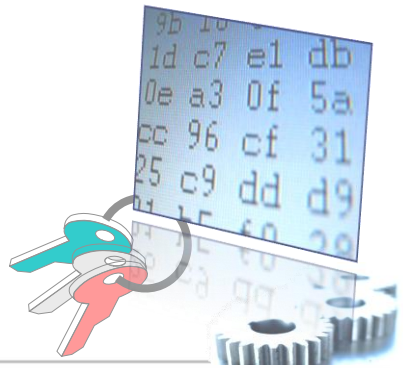


Brute Force Attack: Time to find the key

Remark: The Universe exits since 10^{10} years

Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt

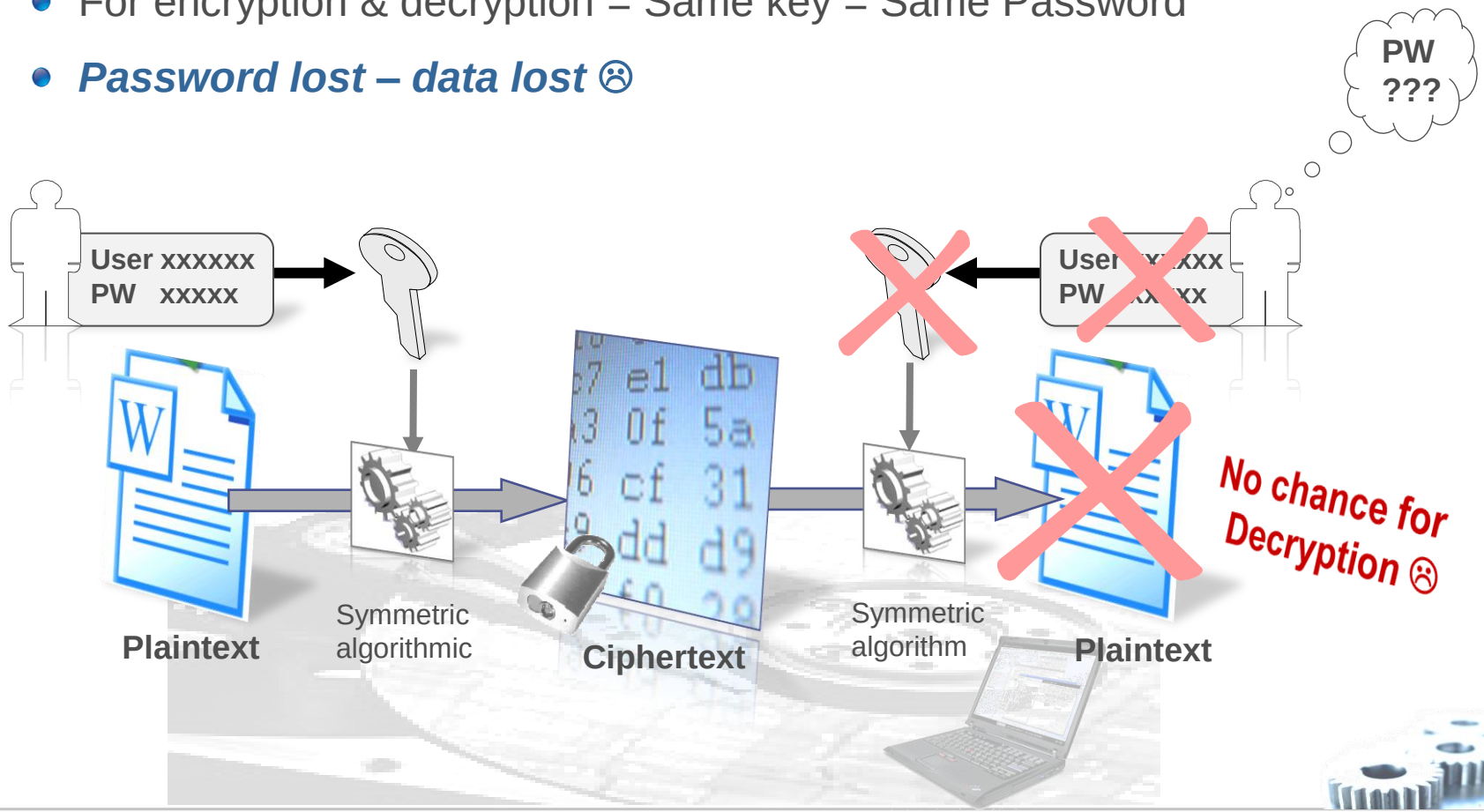


Cryptosystem

Symmetric. Password lost …

Reminder – here we stopped

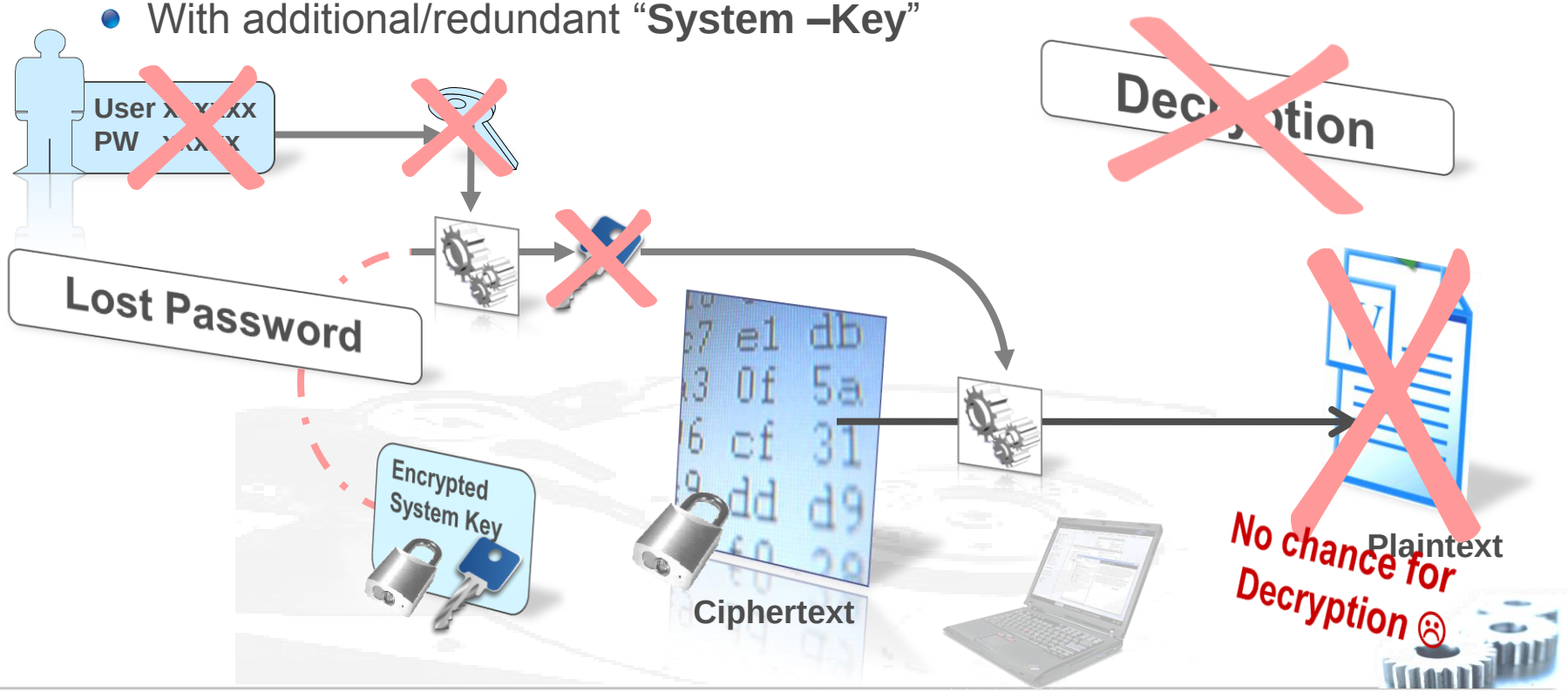
- Principle #1
  - For encryption & decryption = Same key = Same Password
  - ***Password lost – data lost ☹***



Cryptosystem

Symmetric:

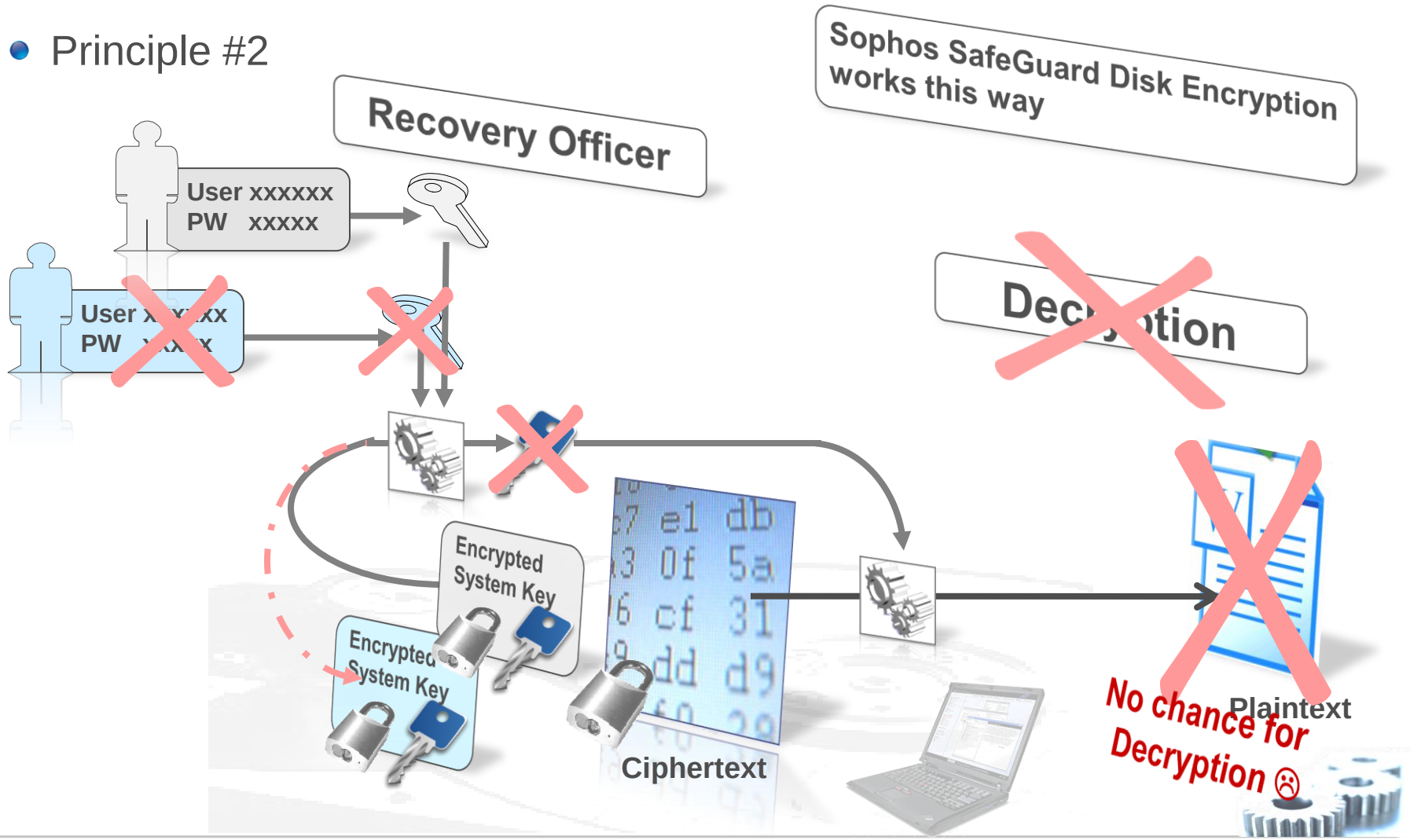
- Principle #2
  - Encryption & **decryption** = Same key = Same Password
  - Key/Password must be kept secret
  - With additional/redundant "**System –Key**"



Cryptosystem

Symmetric: With Key Backup/Key Recovery

- Principle #2

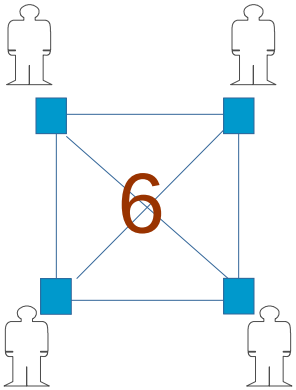


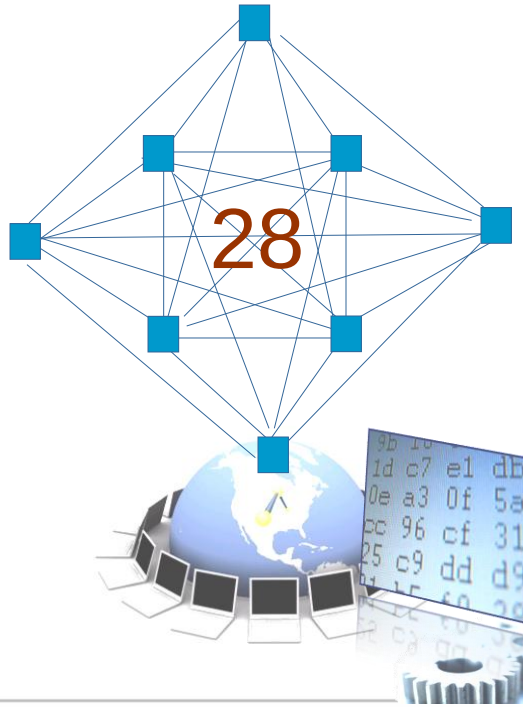
Symmetric Algorithms
Disadvantage

Reminder – here we stopped

- Key Management
  - Symmetric keys will have to be distributed through secure channels = keys must be encrypted
    - Especially in systems with a large number of users (workgroup)
- Example
  - n-partner need
  - n = 4 → 6 keys
  - n = 6 → 15 keys
  - n = 12 → 66 keys
  - n = 1000 → 499500 keys

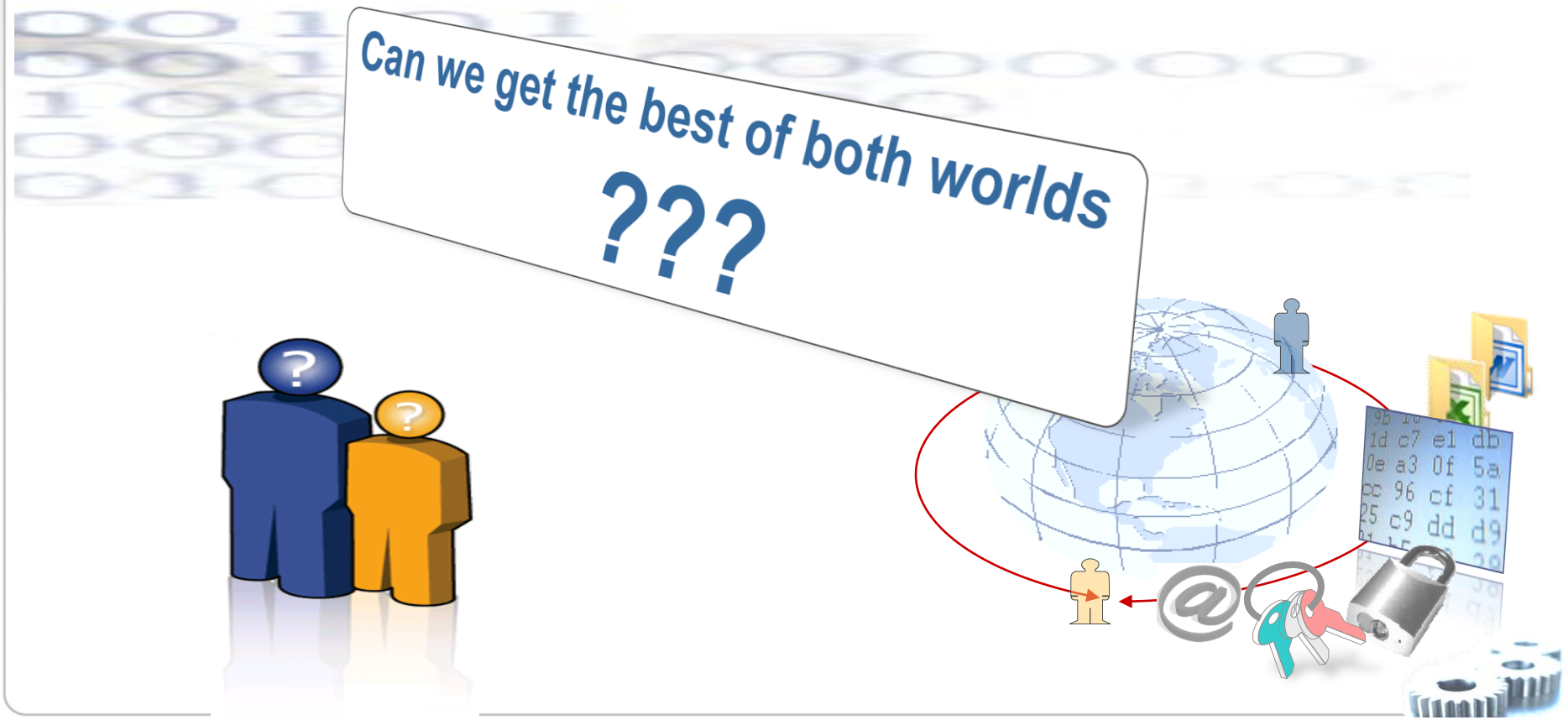
n* (n-1)/2 keys





Cryptosystems
The Challenge

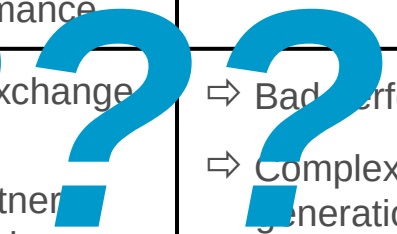
- Asymmetric encryption can offer key management advantages
- Symmetric encryption can offer speed advantages.

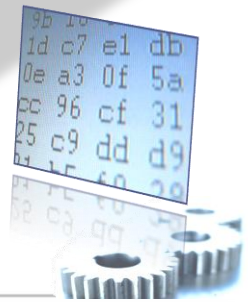


Cryptosystems

Characteristics: Summary

	Algorithms	
	Symmetric (e.g. AES)	**Asymmetric** (e.g. RSA)
Advantage	⇨ Easy key generation (random) ⇨ Good performance	⇨ No key exchange necessary
Disadvantage	⇨ Secret key exchange necessary ⇨ For each partner key is needed n*(n-1)/2	⇨ Bad performance ⇨ Complex key generation
Used for	⇨ Encryption of mass data: Data Confidentiality	⇨ Key management ⇨ Authentication ⇨ Digital Signature



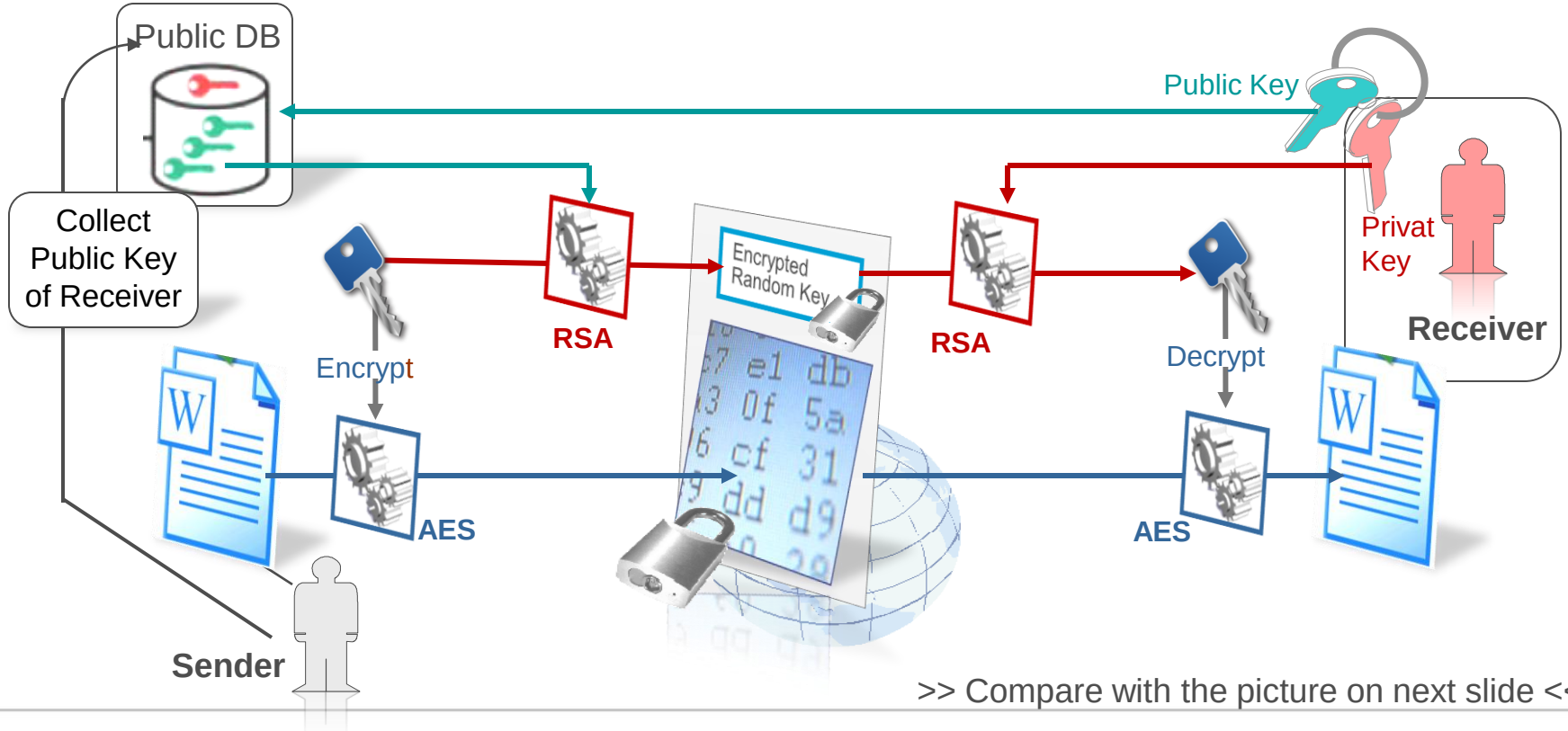


Hybrid Encryption = Digital Envelope

Hybrid Encryption

Mix of Algorithms: Symmetric - Asymmetric

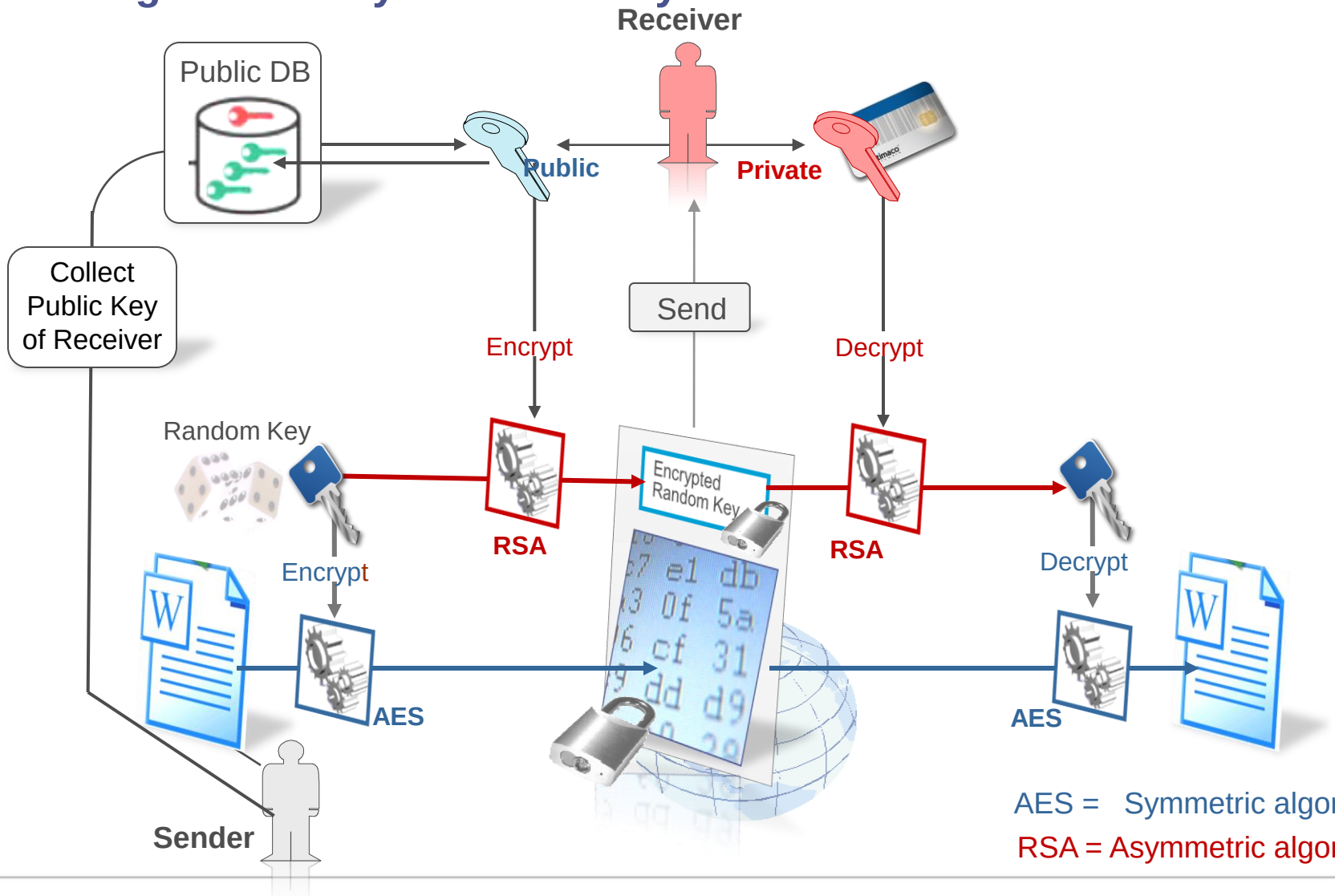
- Because symmetric algorithms work much faster than asymmetric algorithms most cryptosystems use both types = Hybrid Cryptosystems = Digital Envelope



>> Compare with the picture on next slide <<

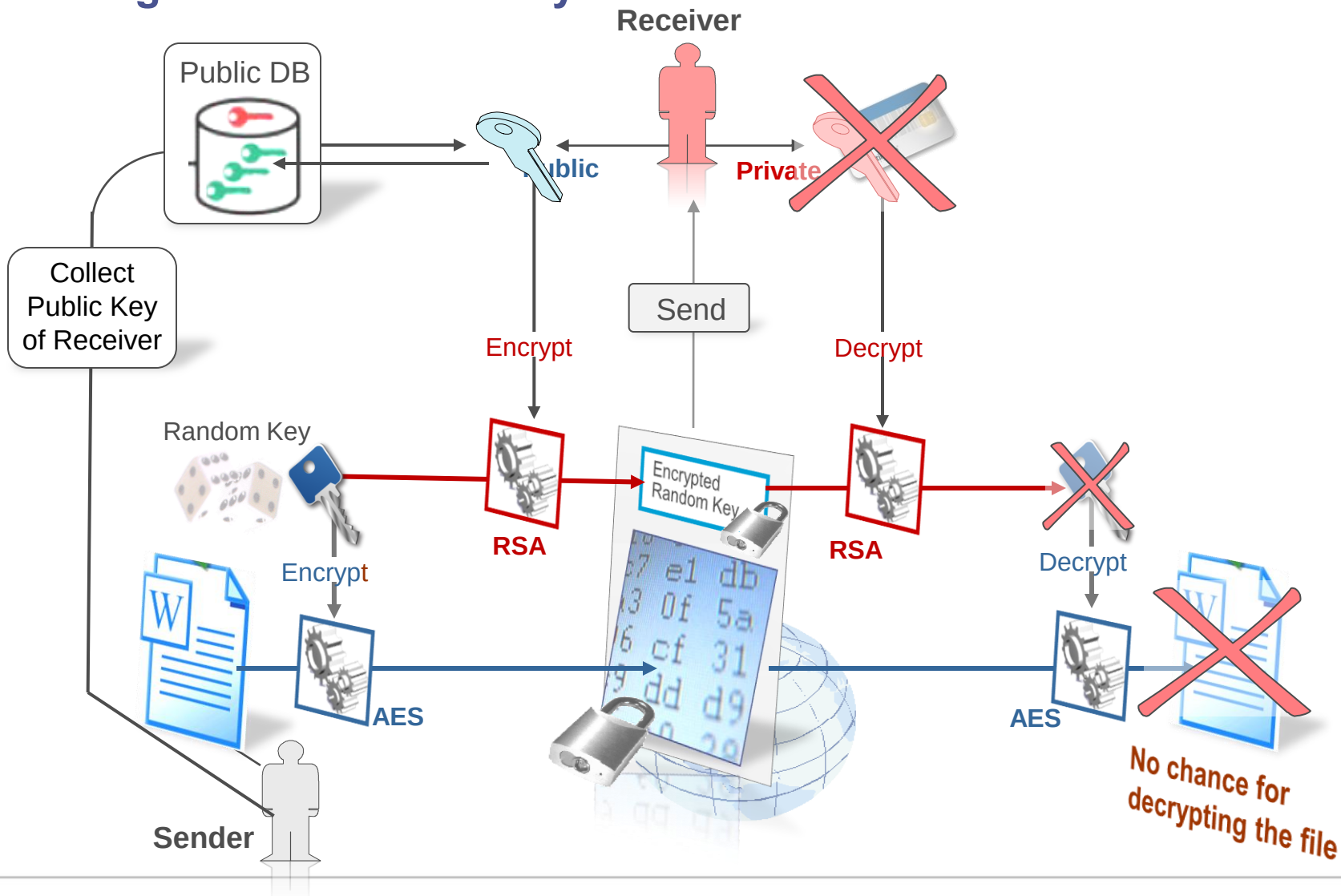
Hybrid Encryption

Mix of Algorithms: Symmetric - Asymmetric



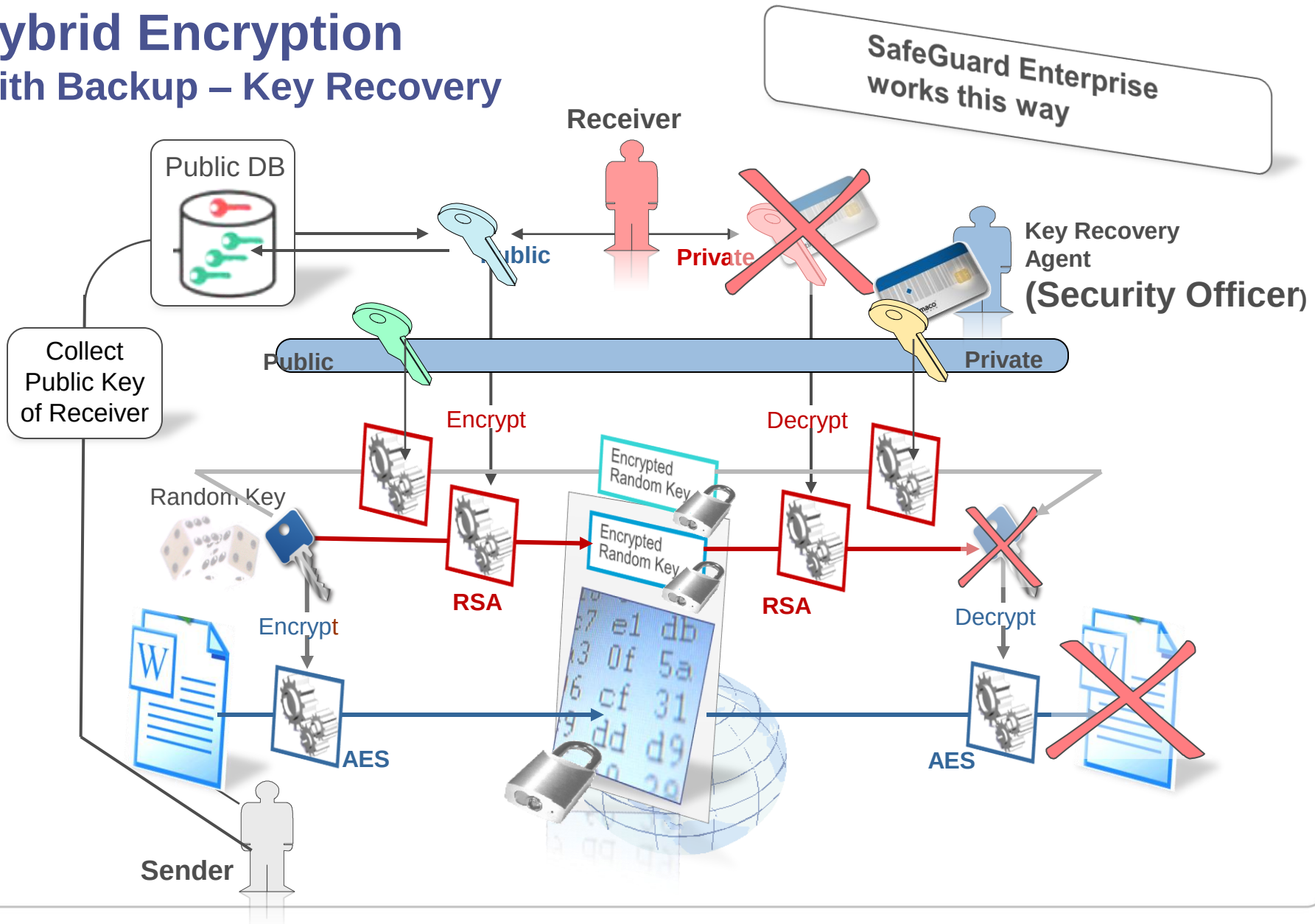
Hybrid Encryption

Mix of Algorithms: Private Key lost ….



Hybrid Encryption

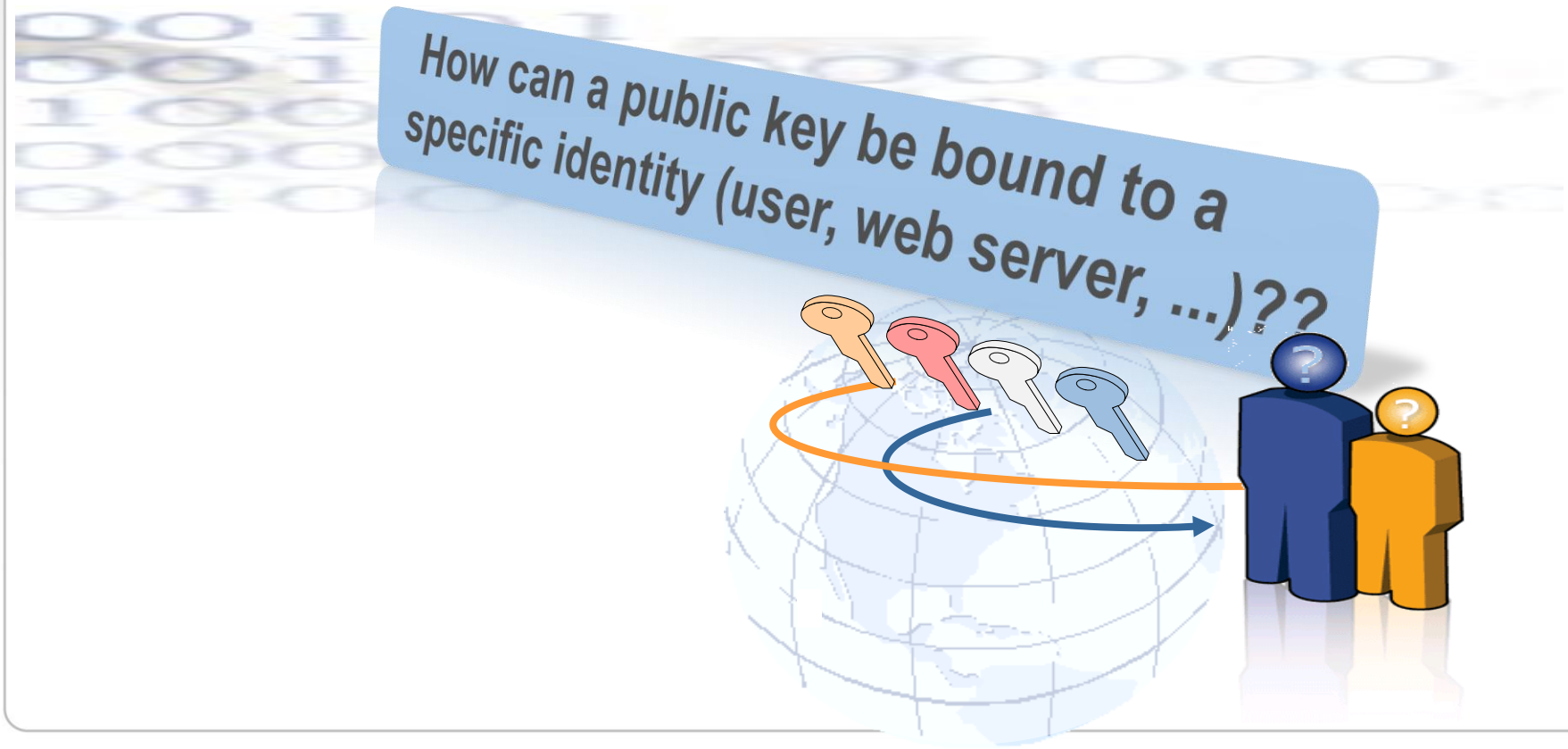
With Backup – Key Recovery



Trust

Based on Public Key Infrastructure (PKI)

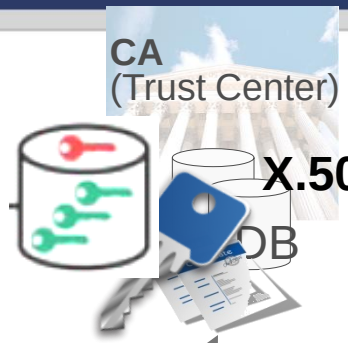
- Which Public Key belongs to which user?
- How can I trust that the key belongs to a user?



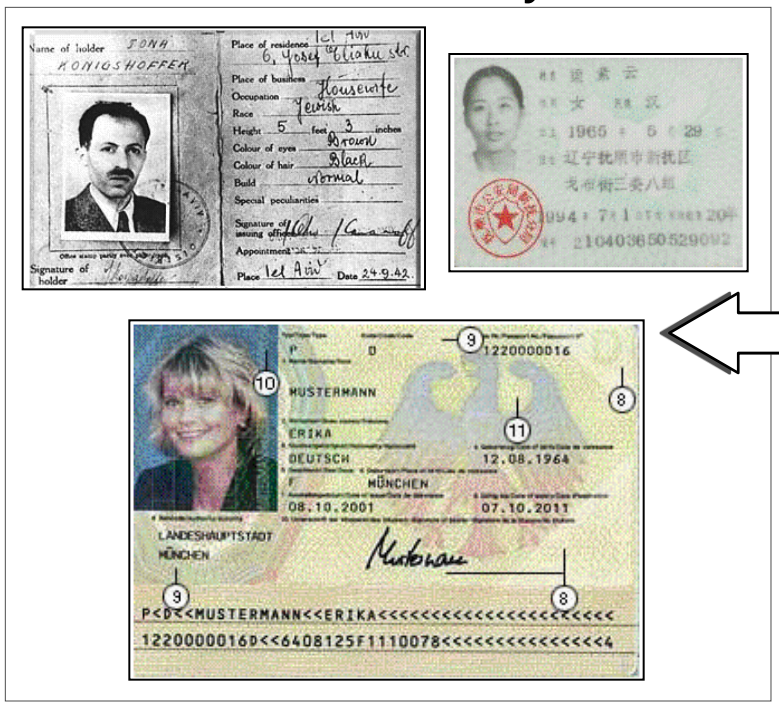
X.509 Certificate

What is it in general?

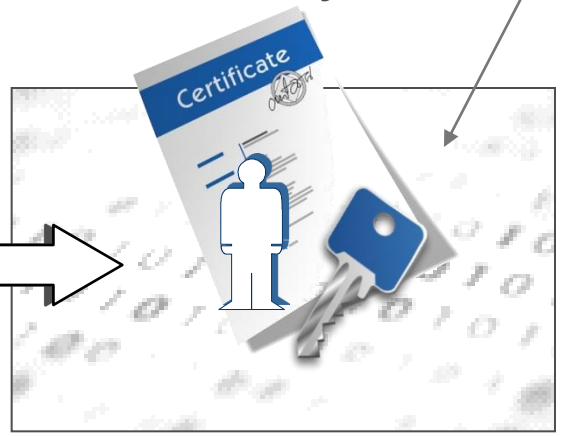
- Trust in Certification Authority (CA) - Trust in Certificates
  - Is a trustworthy institution that verifies public keys
  - Thereby issuing certificates, e.g. VeriSign



Your identity



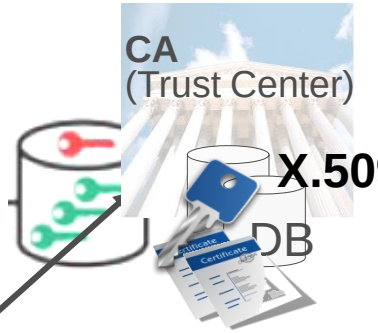
Your digital identity
>> Bits & Bytes <<



X.509 Certificate

Summary

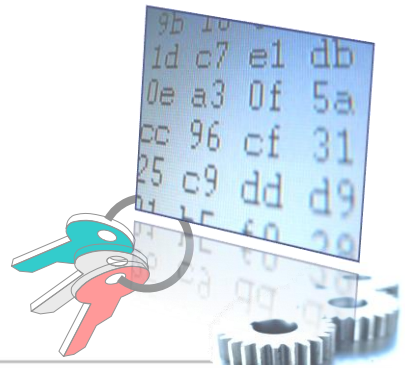
- Main Content



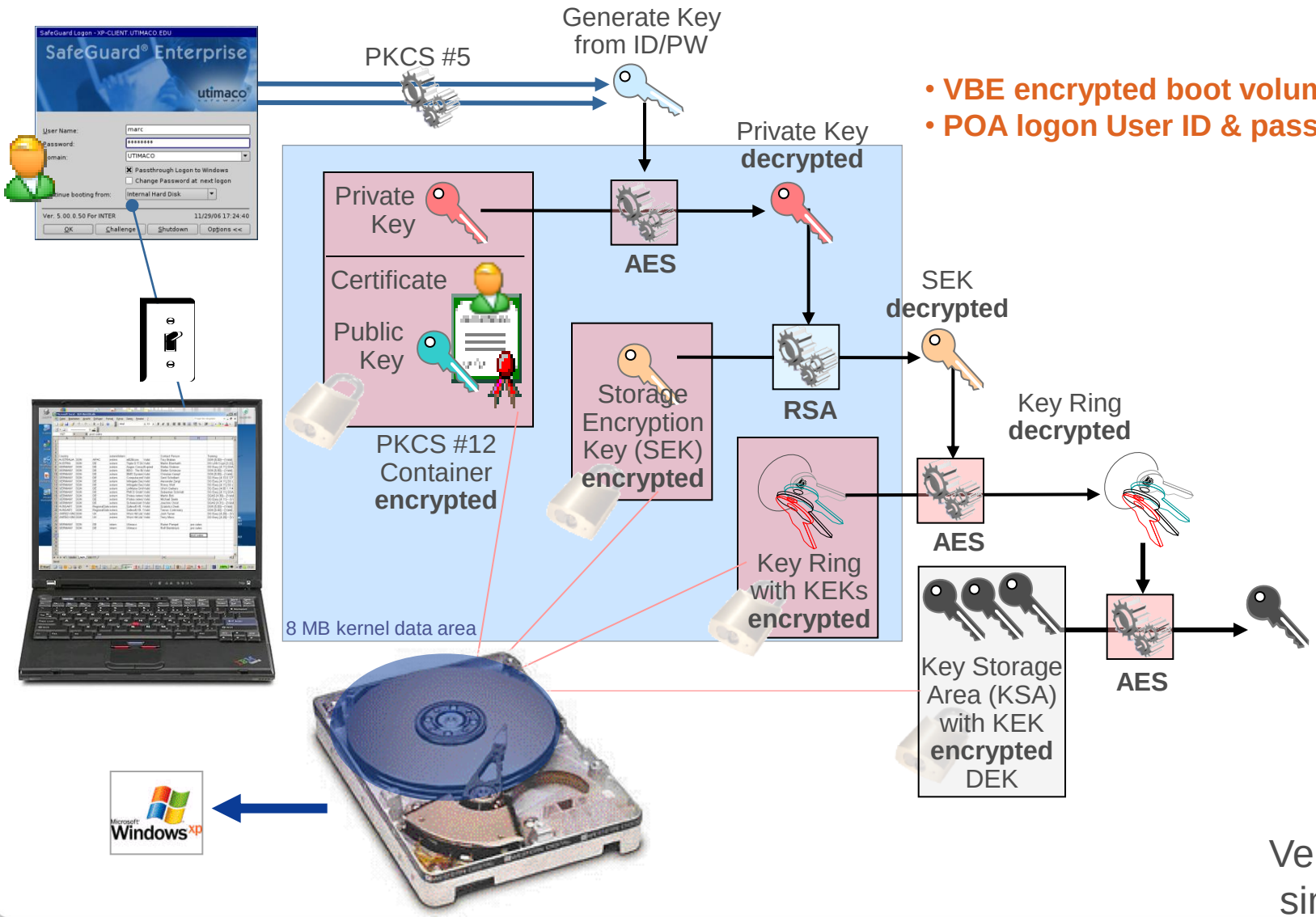
- Issuer (CA/Trustcenter)
- Serial Nr, Algorithms Identifier
- Owner (Username)
- Public Key RSA (Owner)
- Valid (from – until)
- Digital Signature of Issuer (CA/Trustcenter)

Agenda

- Introduction
- Market Pains
  - Risks
  - Negative impacts
- Terminology
  - Basics/ Terminology
  - Secure Key lengths
- Symmetric Algorithms
  - How it works - Characteristics
- Asymmetric Algorithms
  - How it works – Characteristics
- Cryptosystems in Practice
  - Key Backup/ -Recovery
  - Hybrid encryption
  - X.509 Certificates
- Market products
  - Safeguard Enterprise
  - Safeguard LanCrypt



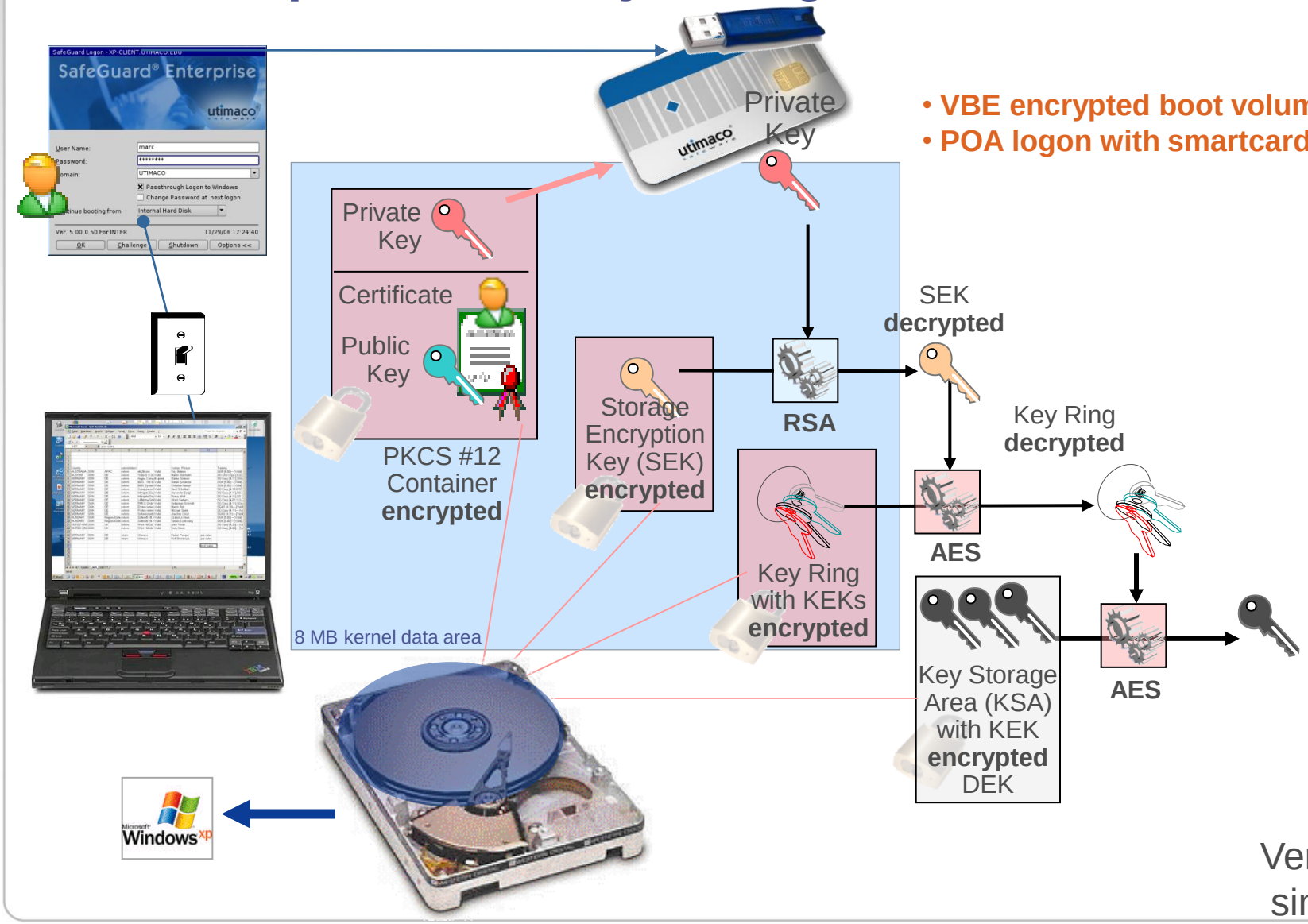
SGN boot process - Keymanagement



- **VBE encrypted boot volume**
- **POA logon User ID & password**

Very much simplified

SGN boot process - Keymanagement



- **VBE encrypted boot volume**
- **POA logon with smartcard/token**

Very much simplified

Keymanagement / Transparent encryption

- DEK?
- KEK?
- KSA?

Keymanagement / Transparent encryption

- Data is encrypted with a random Data Encryption Key (DEK)
- DEKs are encrypted with Key Encryption Keys (KEKs)
- Every SGN object (OU, domains, users groups, users) have their KEKs assigned in the database
- KEKs can be assigned to other objects if necessary, e.g.
  - … if users from different departments want to share encrypted data
  - … if the data on an encrypted disk needs to be recovered
  - …

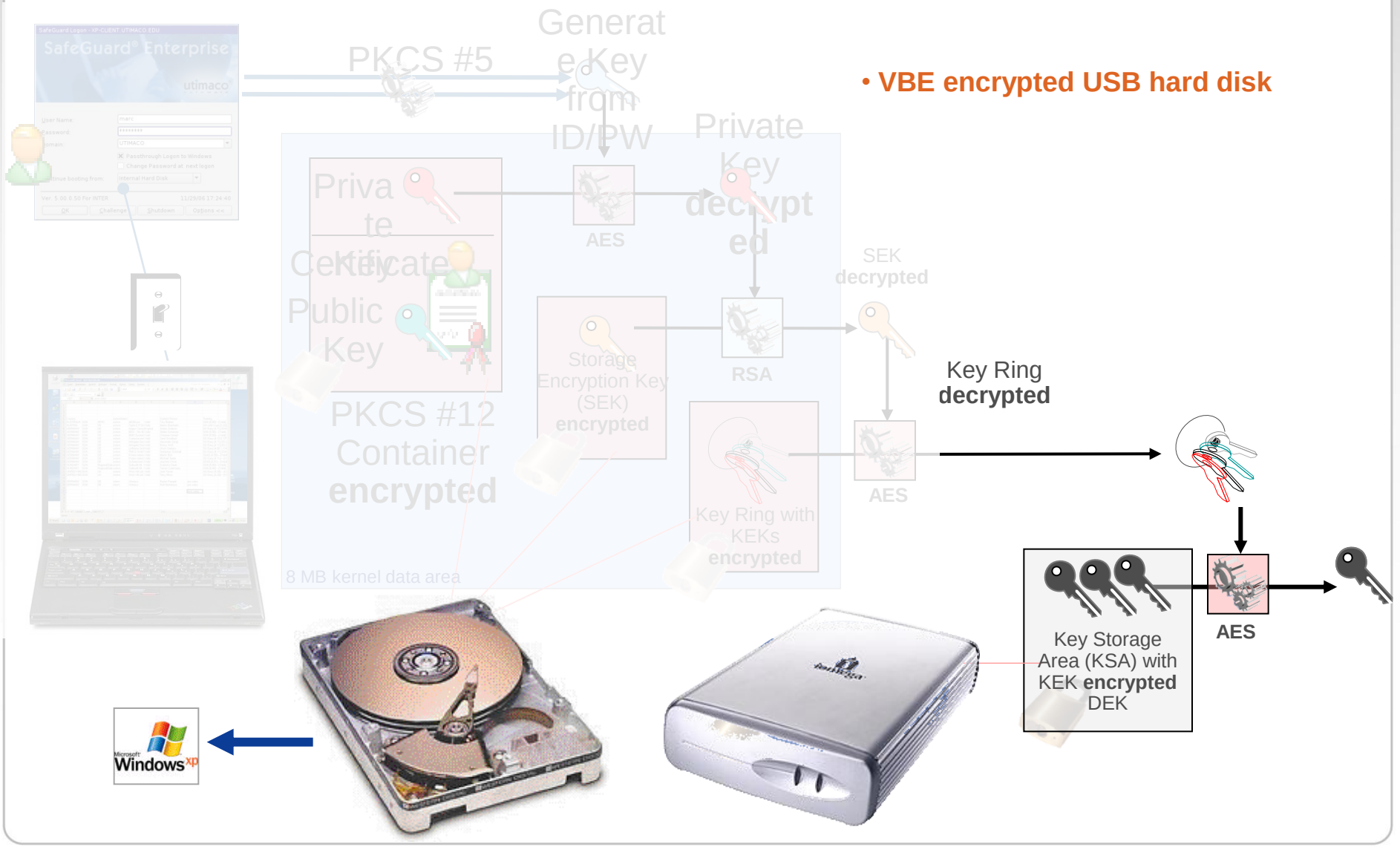
SGN boot process / Key Storage Area

- Volume based encryption stores information about used Key Encryption Keys (KEKs) in Key Storage Areas (KSAs)
- Every volume based encrypted device has one KSA and a copy of it

- Users receive their KEKs in a Keyring during logon
- A KEK decrypts the DEK
- The DEK decrypts the data
- The is always only one DEK for a volume
- The DEK is encrypted be at least one KEK or several KEKs
- Boot volumes can only be encrypted volume based

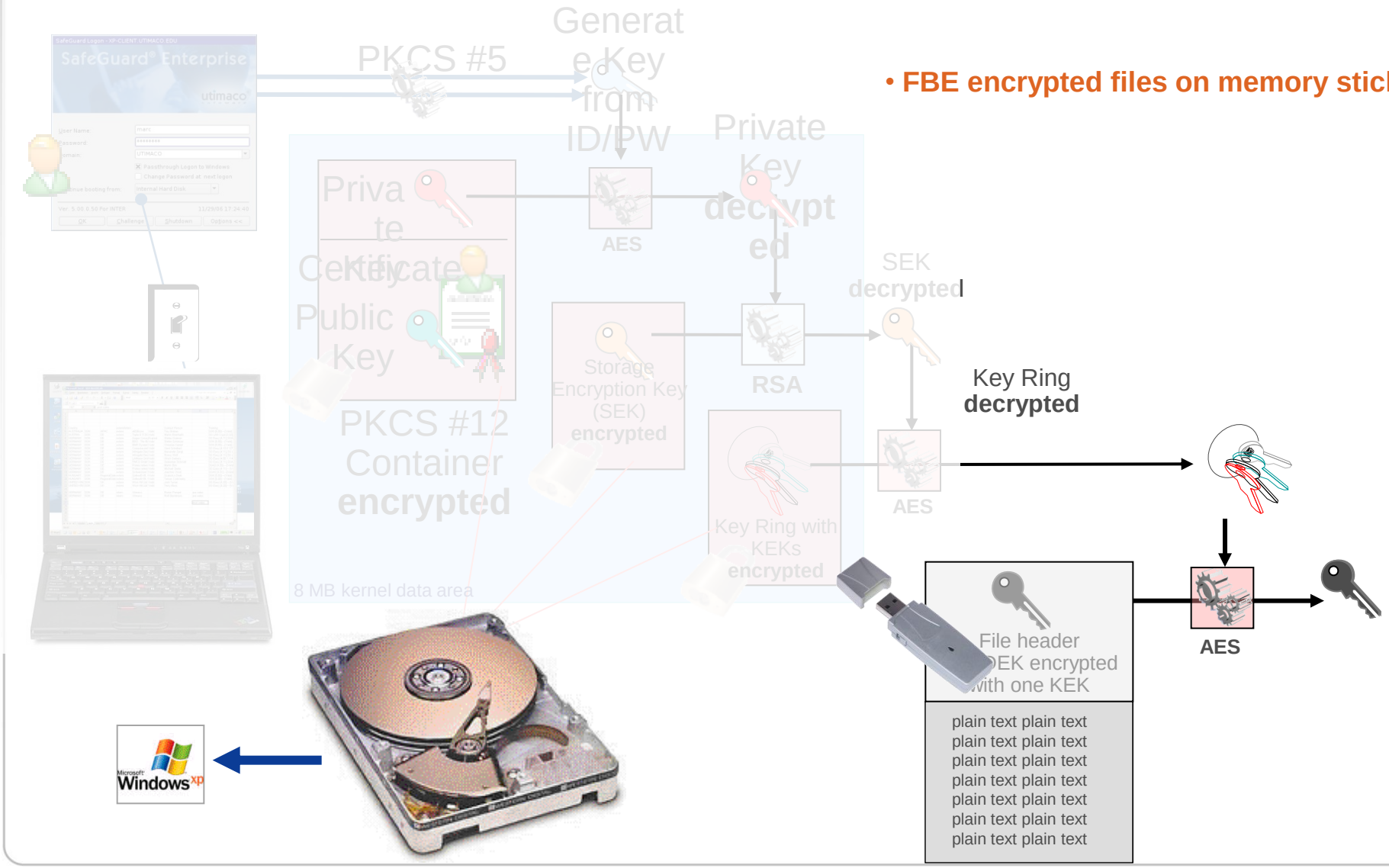
Keymanagement – volume based encryption

- **VBE encrypted USB hard disk**



File header – file based encryption

- **FBE encrypted files on memory stick**

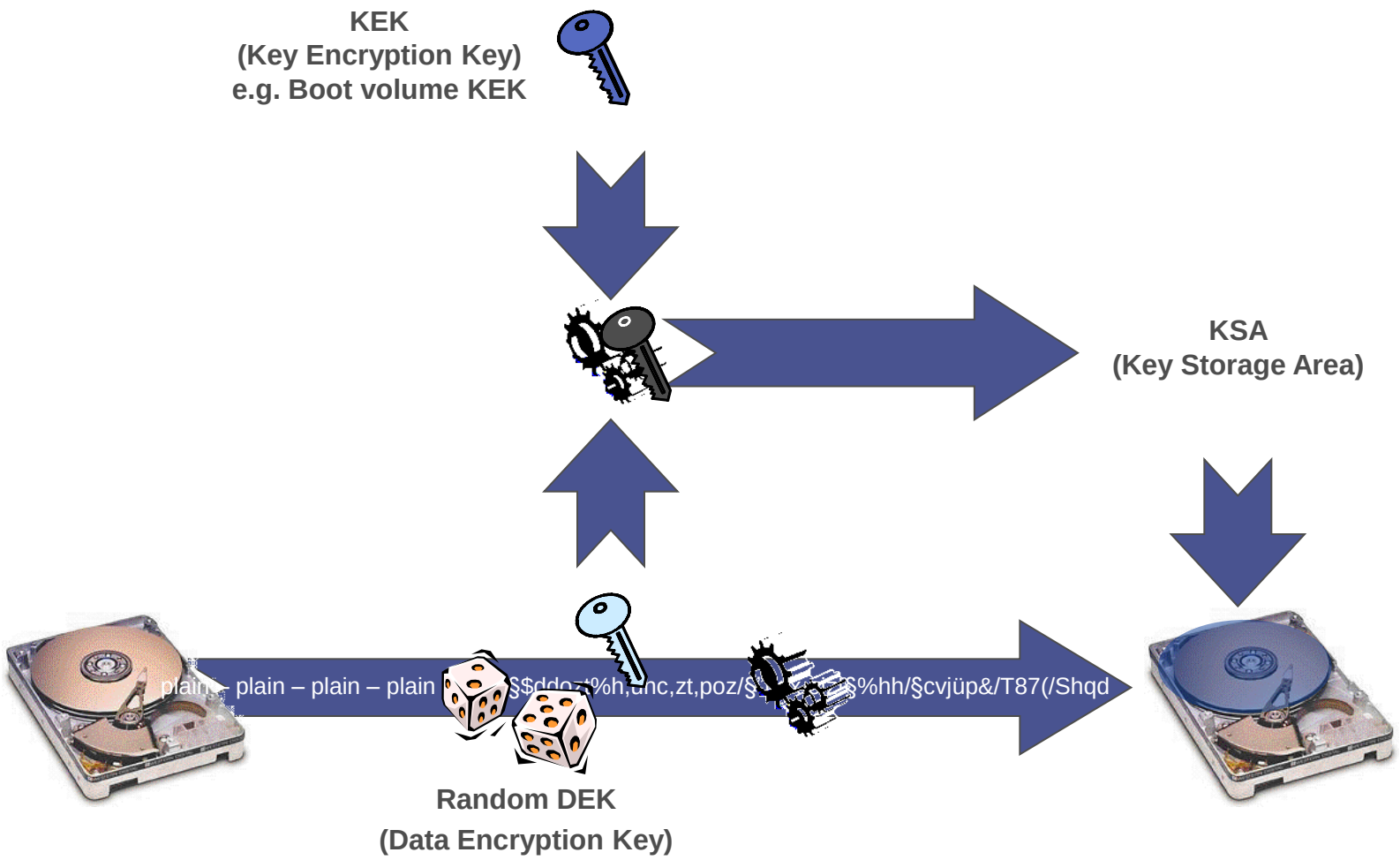


Transparent encryption

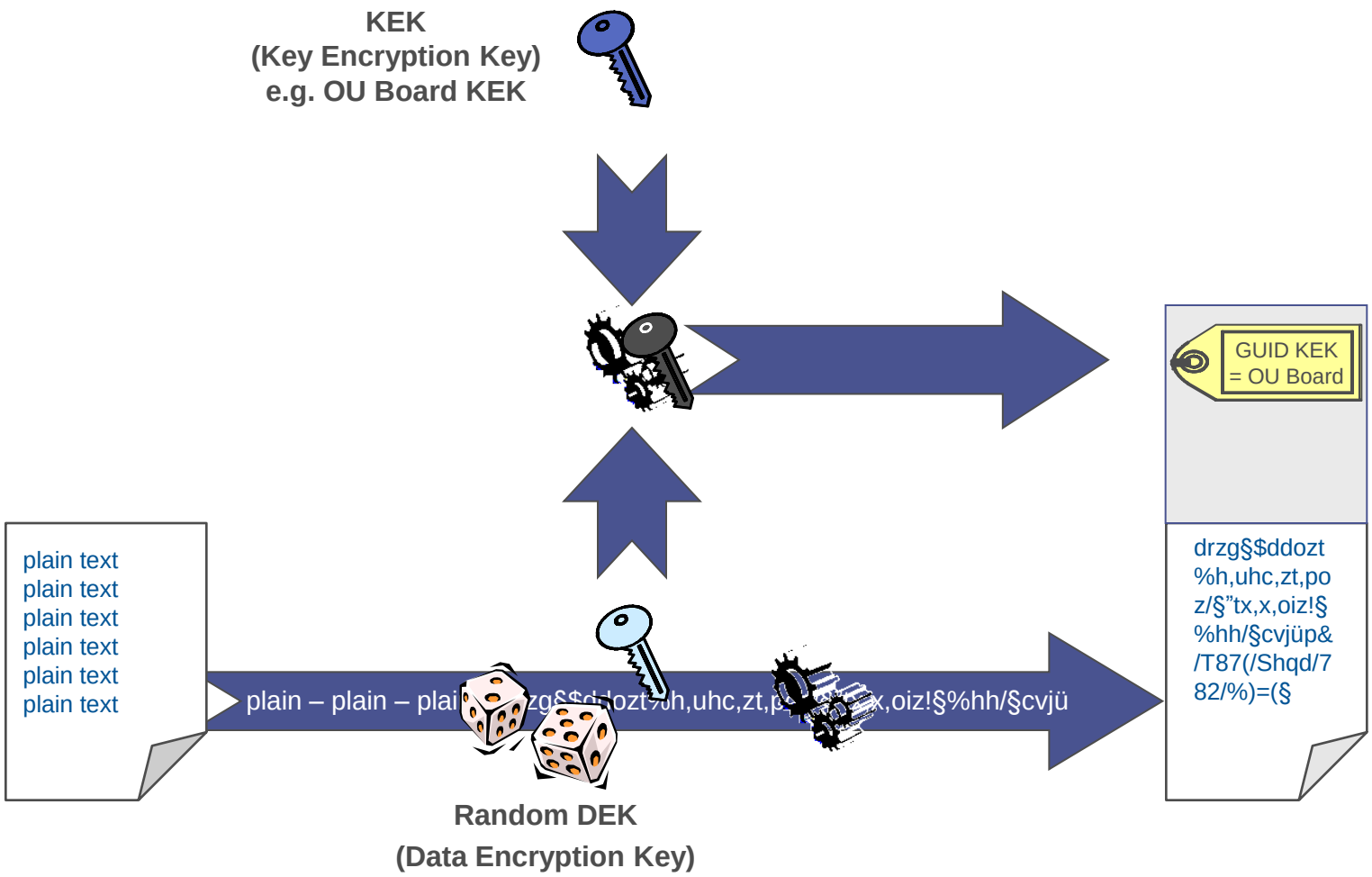
- Volume based vs. File based encryption

	Volume based	File based
Key storage	Key Storage Area for every single volume	File header for every single file
Encryption key used	Random Data Encryption Key (DEK)	Random Data Encryption Key (DEK)
DEK security	Multiple Key Encryption Keys (KEKs) encrypt the DEK	Only one single Key Encryption Key (KEK) encrypts the DEK
KEK storage	User keyring	User keyring

Transparent volume based encryption

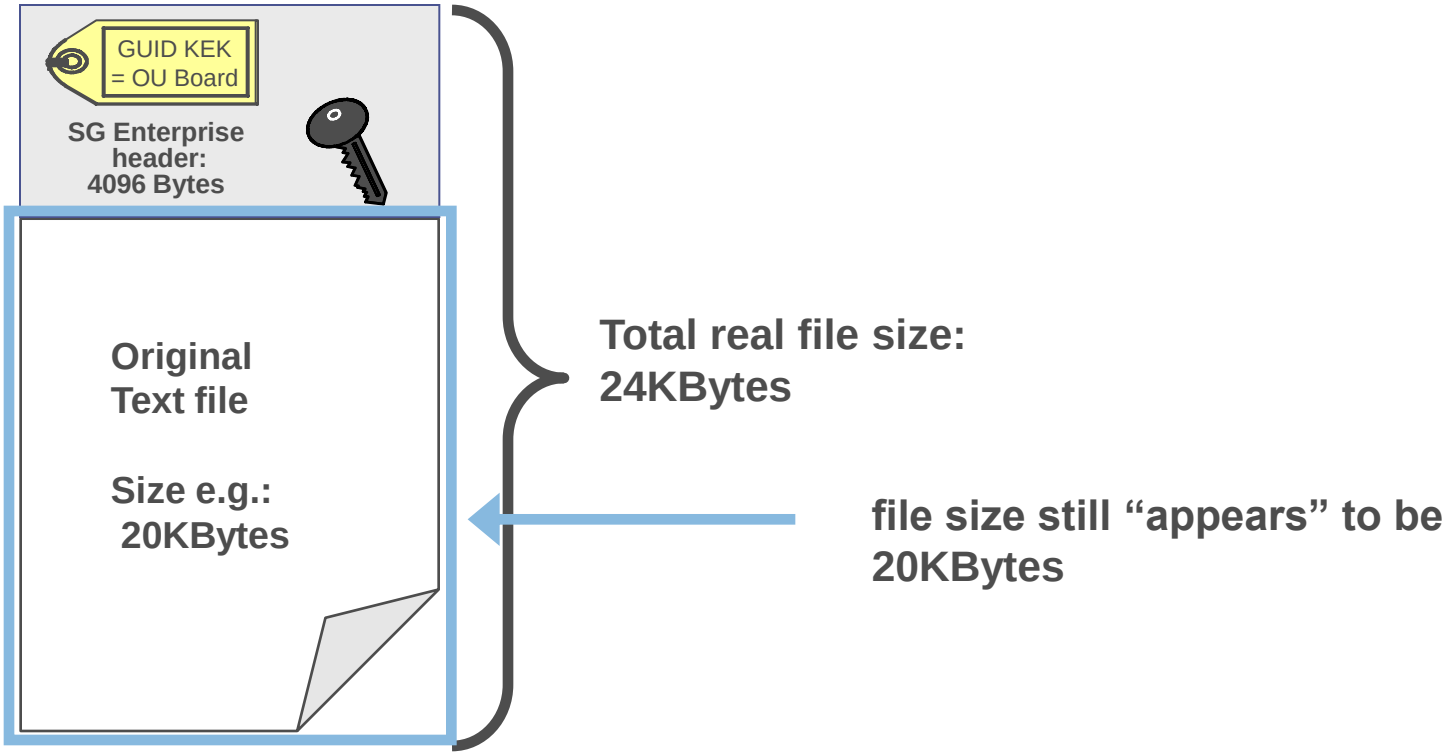


Transparent volume based encryption

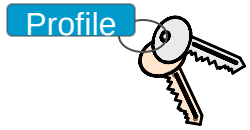


Transparent file based encryption driver

- SGN file based encryption changes the file size
  - because it adds a 4096 bytes header to each file
- File size correction “fakes” original file size



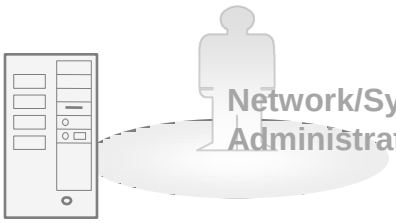
Profiles in distributed file encryption



HR

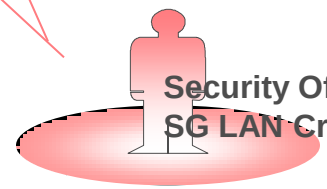
Big Boss

Sales Director



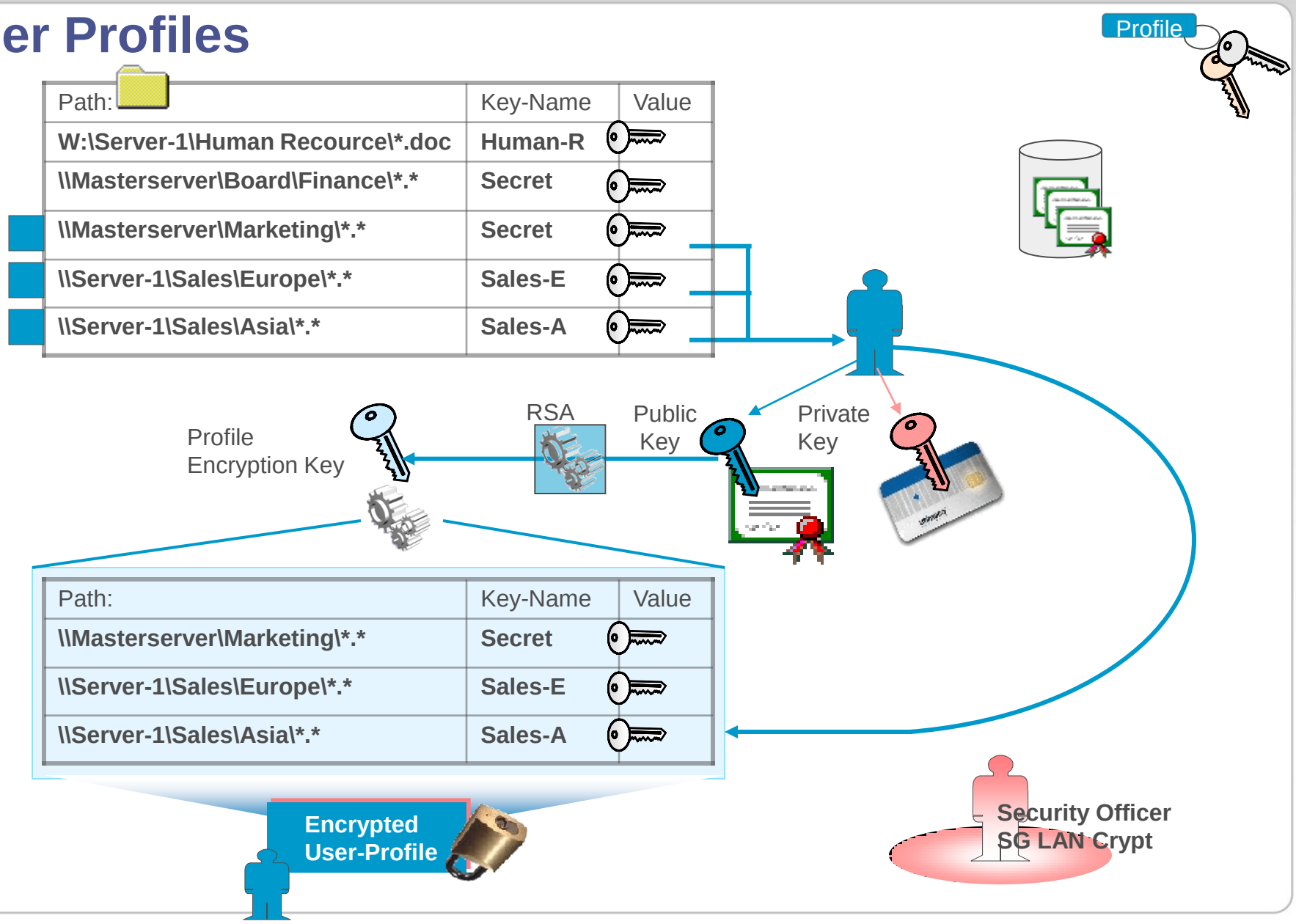
Network/System Administrator

Typical tasks:
- Administration of users and groups
- Administration of file system
- Access control, Backup

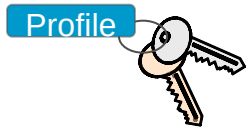


Security Officer
SG LAN Crypt

User Profiles

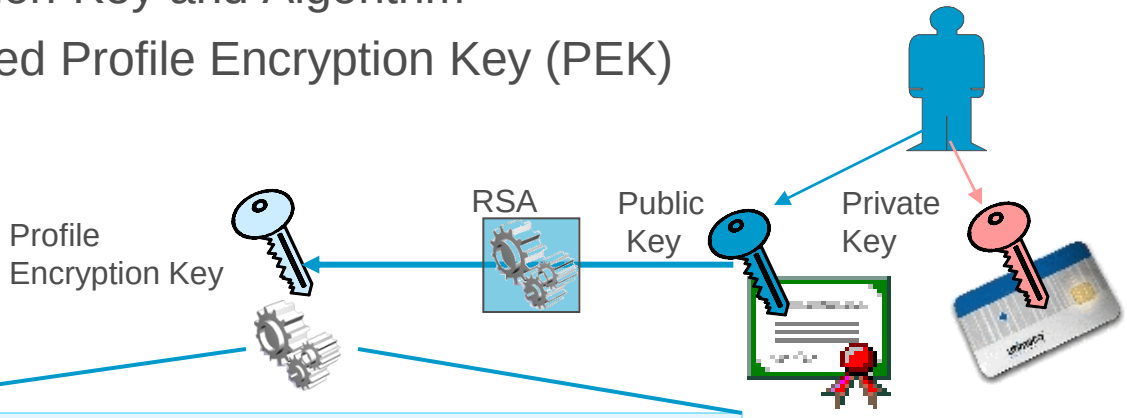


User Profiles



All Users get a „profile“, which contains the encryption rules

- Path/Directory
- Files (Extension, Wildcards)
- Encryption-Key and Algorithm
- Encrypted Profile Encryption Key (PEK)

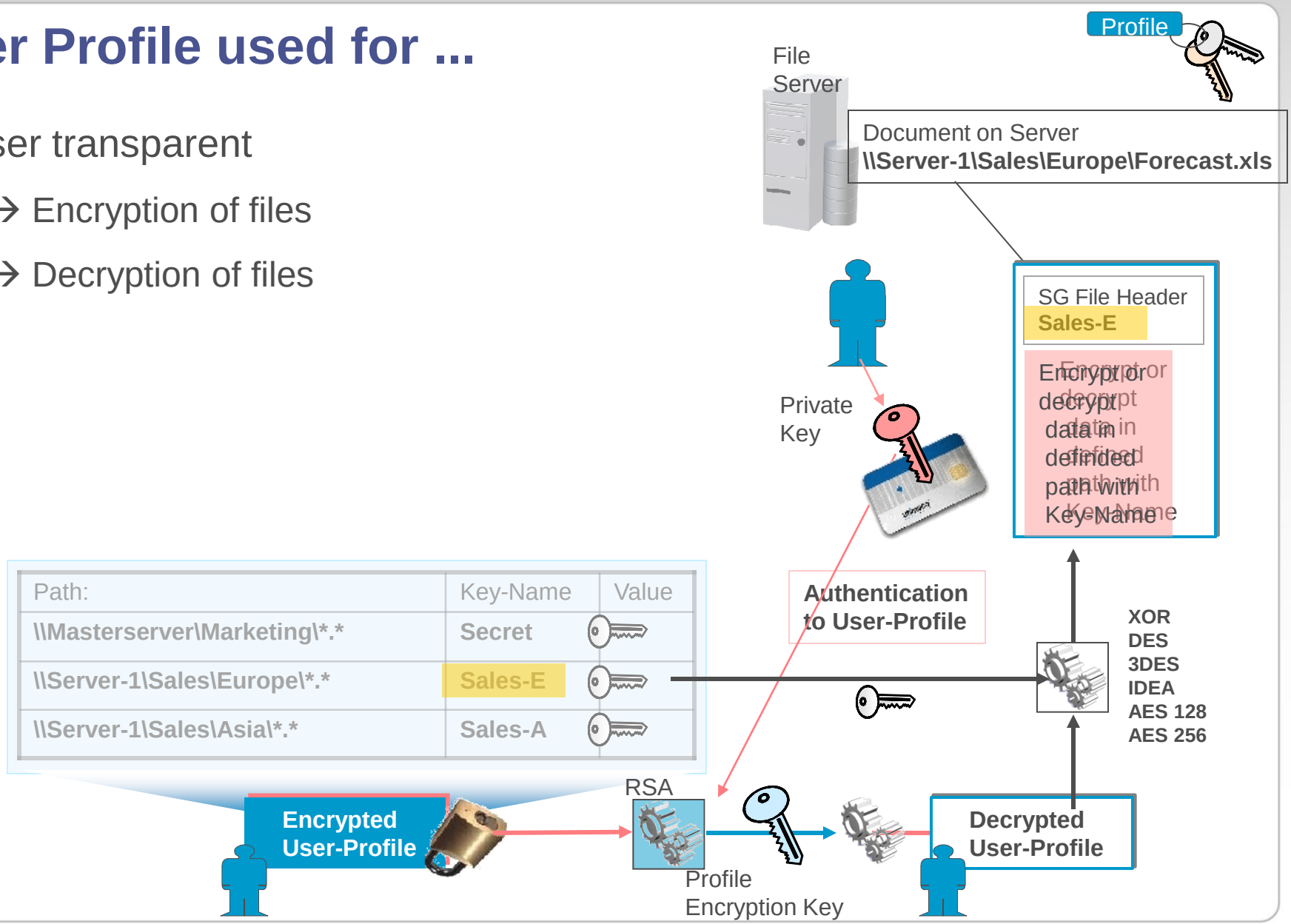


Path:	Key-Name	Value
\\Masterserver\Marketing*.*	**Secret**	
\\Server-1\Sales\Europe*.*	**Sales-E**	
\\Server-1\Sales\Asia*.*	**Sales-A**	

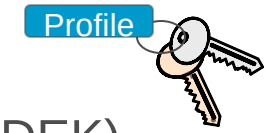
SO encrypts User profiles with users Public Key

User Profile used for ...

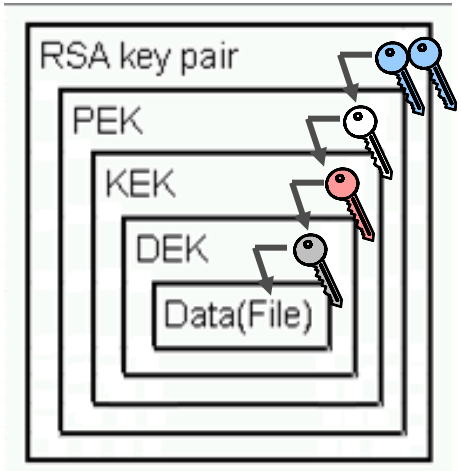
- User transparent
  - → Encryption of files
  - → Decryption of files



Key Management Concept



- Content of file is encrypted with a symmetric *Data Encryption Key* (DEK),
  - **DEK** gets encrypted with a *Key Encryption Key* (**KEK**)
  - The **KEK** is assigned to a specific SGLC user group to encrypt files. It's taken from the SGLC **profile**.
  - Profiles for each user are encrypted with a user-specific *Profile Encryption Key* (**PEK**).
  - **PEK** in turn is encrypted with the user's **public key**.

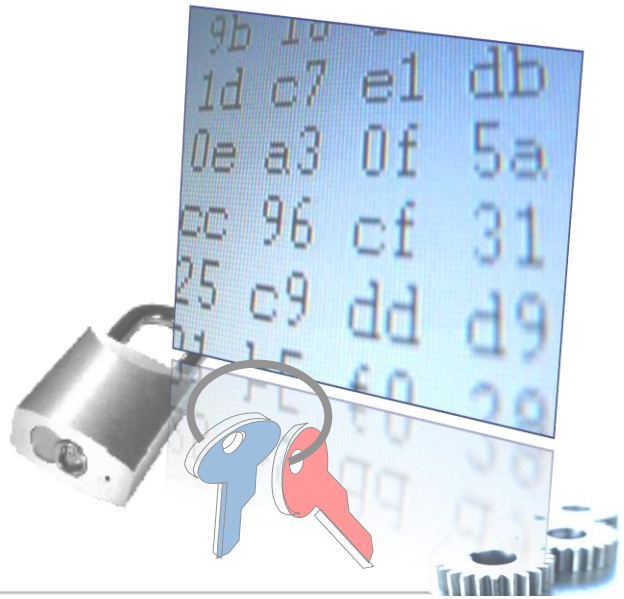


- DEKs and PEKs are generated **randomly** each time a new one is needed.
- KEKs are generated by the SG LAN Crypt administrator
  - Stored in the administration database (secured by the Security officer key pair)
  - Data Recovery possible in case of the user looses his Keys (KEKs).

Keyname	Long keyname	Algorithm	Enabled
MARKETING_GENERA	Marketing generall	AES256	Enabled
GREEN_BANNANAS	Green Bannanas	AES256	Enabled
SALES	Sales	AES256	Enabled

Questions …

Feedback session



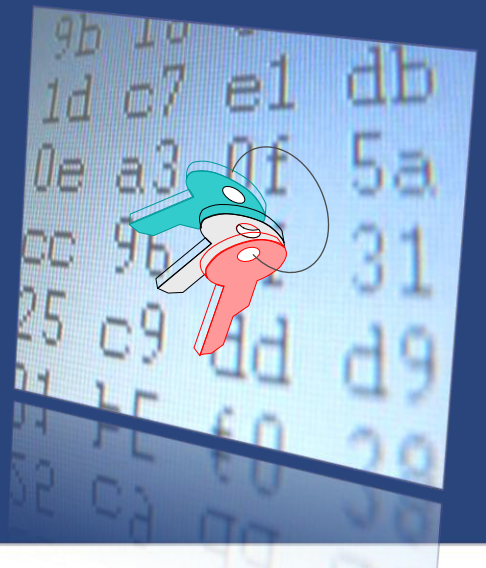
Thank You

Luca Mairani

Sales Engineer

SOPHOS ITALIA

luca.mairani@sophos.it



Link per approfondimenti

- Ricerca Ponemon Institute 2010: http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf
- Portale crittografia Wikipedia: http://it.wikipedia.org/wiki/Portale:Crittografia
- Crittografia simmetrica: http://it.wikipedia.org/wiki/Crittografia_simmetrica
- AES: http://it.wikipedia.org/wiki/Advanced_Encryption_Standard
- Crittografia asimmetrica: http://it.wikipedia.org/wiki/Crittografia_asimmetrica
- RSA: http://it.wikipedia.org/wiki/RSA
- Differenze e crittosistemi ibridi: http://it.wikipedia.org/wiki/Differenza_fra_cifratura_simmetrica_e_asimmetrica
- Interessante studio sulla crittografia ibrida: http://www.iacr.org/archive/crypto2004/31520425/crypto-hybrid-04.pdf
- Prodotti Sophos Encryption: http://www.sophos.it/products/enterprise/encryption/