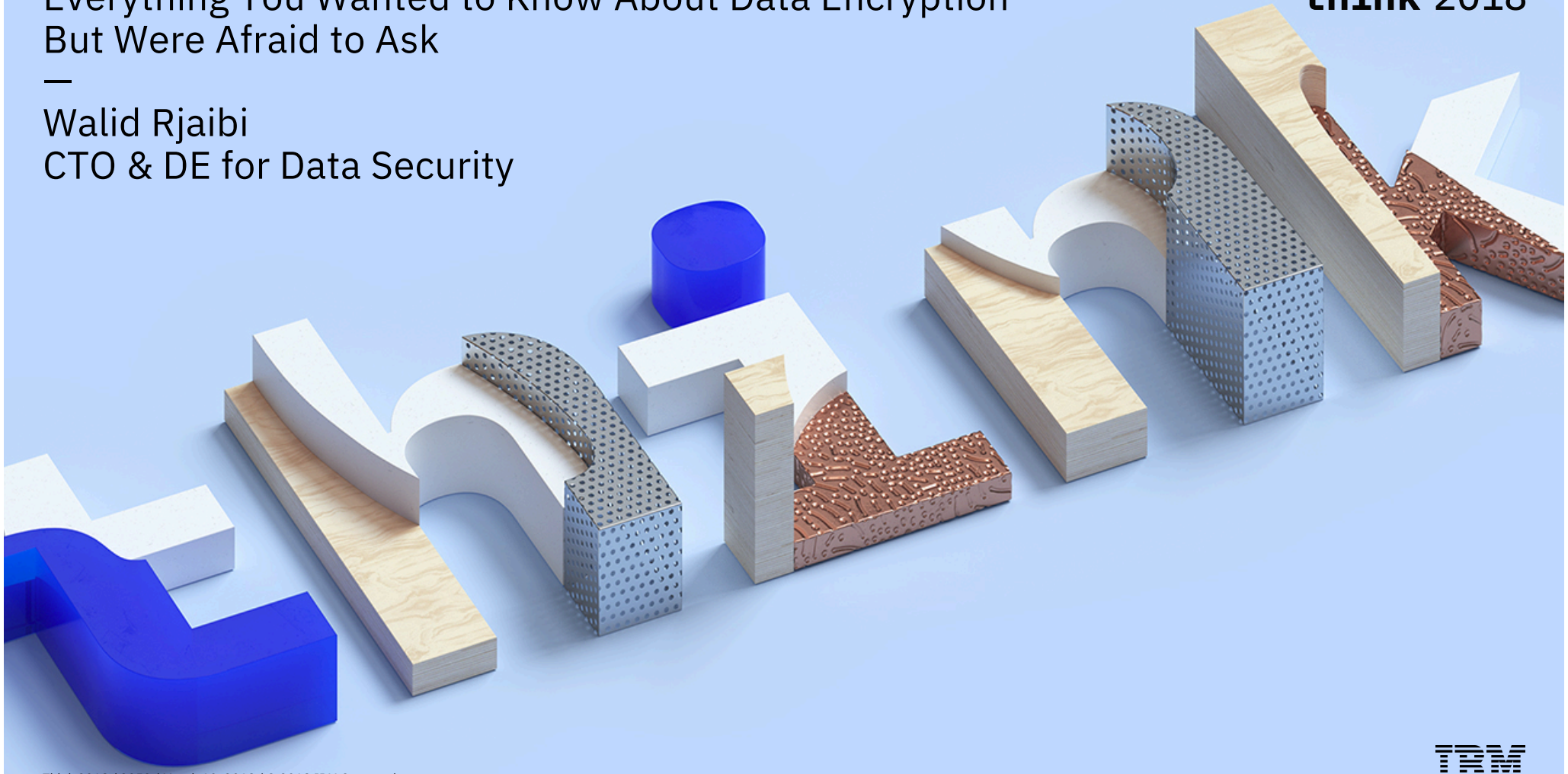
Everything You Wanted to Know About Data Encryption But Were Afraid to Ask

—

Walid Rjaibi
CTO & DE for Data Security

think 2018



IBM

Data Encryption

- The process of encoding data so that only users who have access to the decryption key can decode it

EXAMPLE

Original Value	Encrypted Value
4536 6382 9896 5200	1@#43$%!xy1K2L4P

- Many solutions; how do you choose?

Database Encryption
Column
Tablespace
Database

File System Encryption
Native
Agent-based

Disk Encryption
Volume
Partition
Self-Encrypting Disks (SED)

Symmetric Encryption Algorithms

- **Use the same key for encryption & decryption**
  - AES and 3DES are most commonly used examples

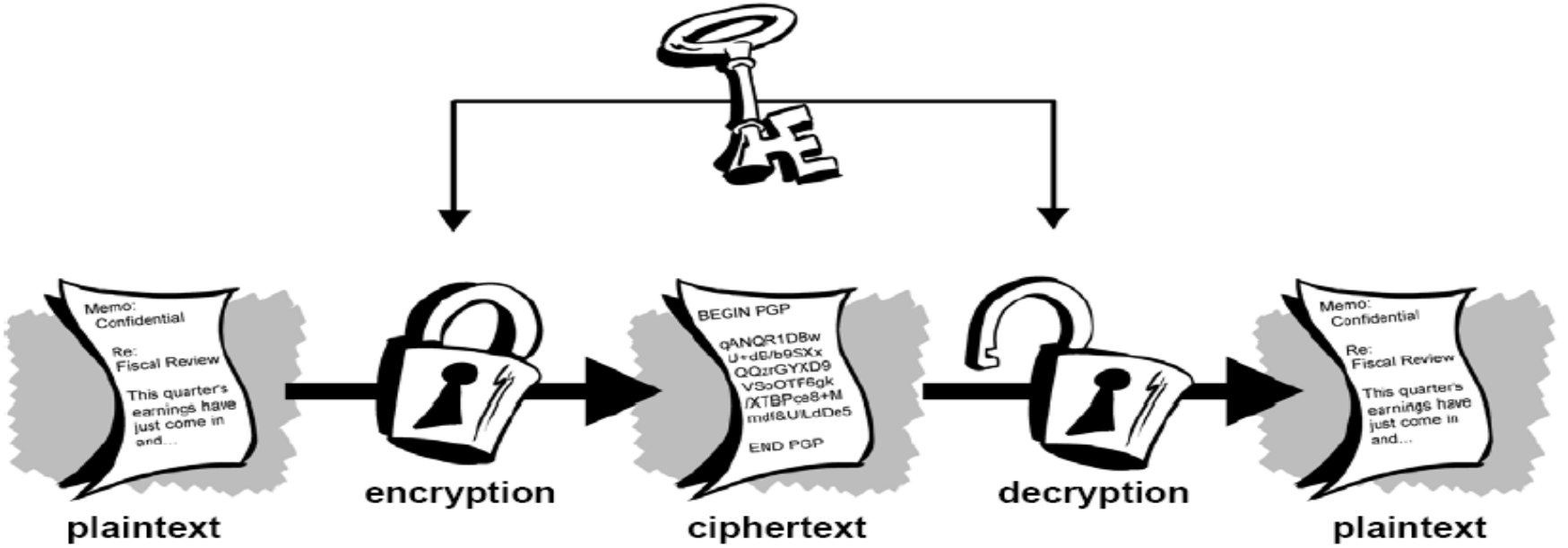


Image source: https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/

Asymmetric Encryption Algorithms

- **Use different keys for encryption & decryption**
  - RSA, ECC, DH are most commonly used examples

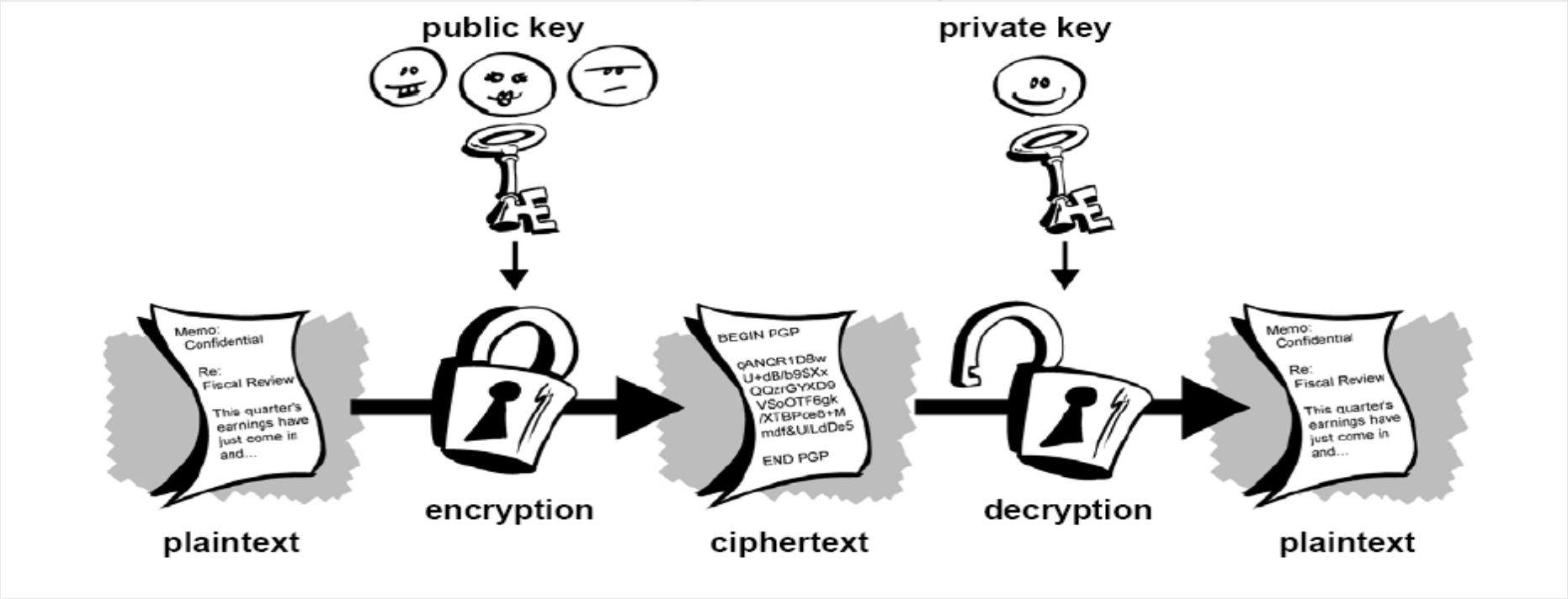
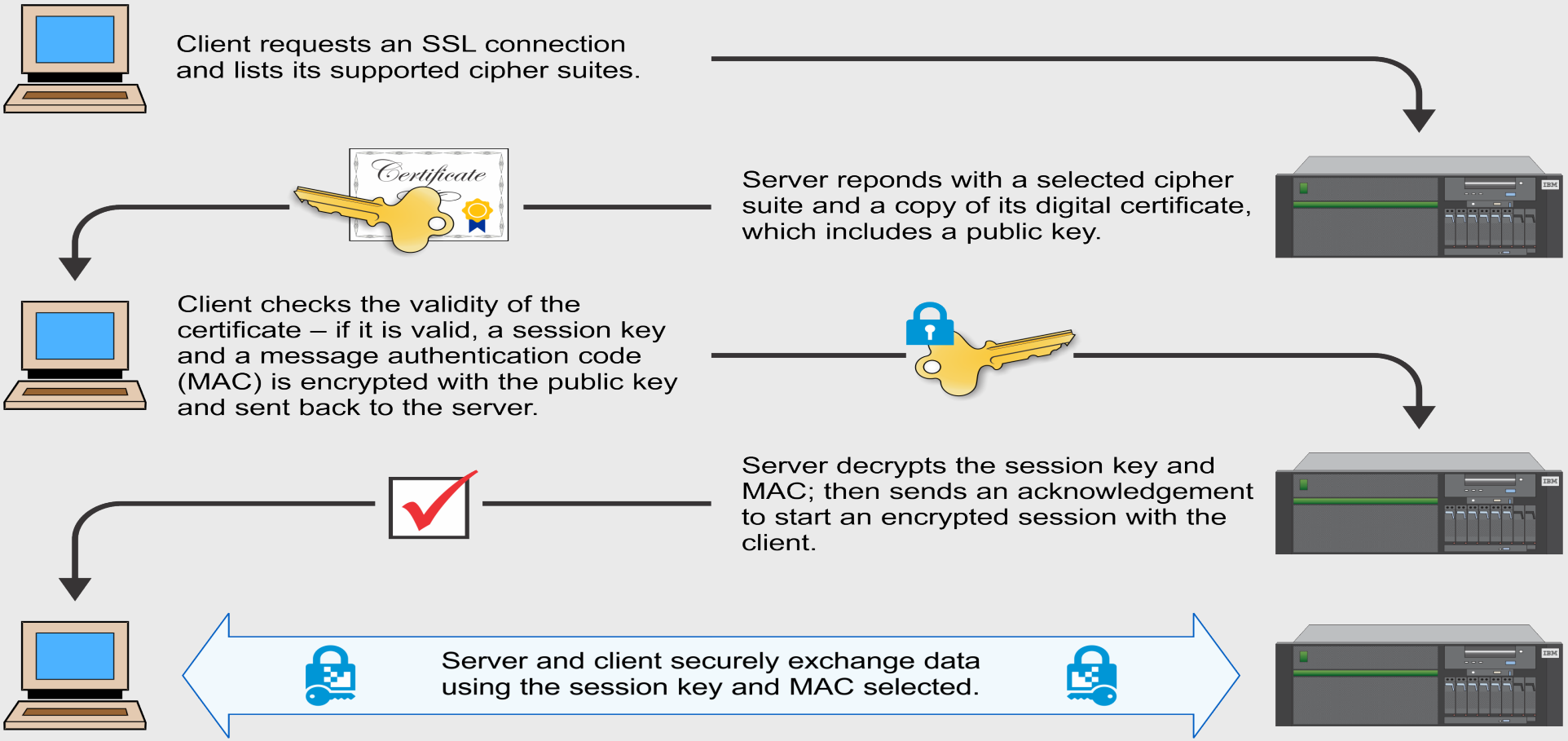


Image source: https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/

Approximate Equivalence in Security Strength

Symmetric key length (AES)	Asymmetric key length (RSA)	Asymmetric key length (ECC)
-	1024	160
-	2048	224
128	3072	256
192	7680	384
256	15360	512

SSL: An Example Where Symmetric & Asymmetric Encryption Are Combined



Key Management

- Refers to the management of encryption keys throughout their life cycle
- Multiple options exist, depending on the encryption solution

Keystores

A password-protected file with a format for storing encryption keys

KMIP Servers

A dedicated server for centrally managing encryption keys across the enterprise

HSM Appliances

A hardened appliance dedicated to storing encryption keys

Cloud KMS

A cloud key management service typically for managing keys used by other cloud services

Encryption Solution Example: DB2 Native Encryption / KMIP

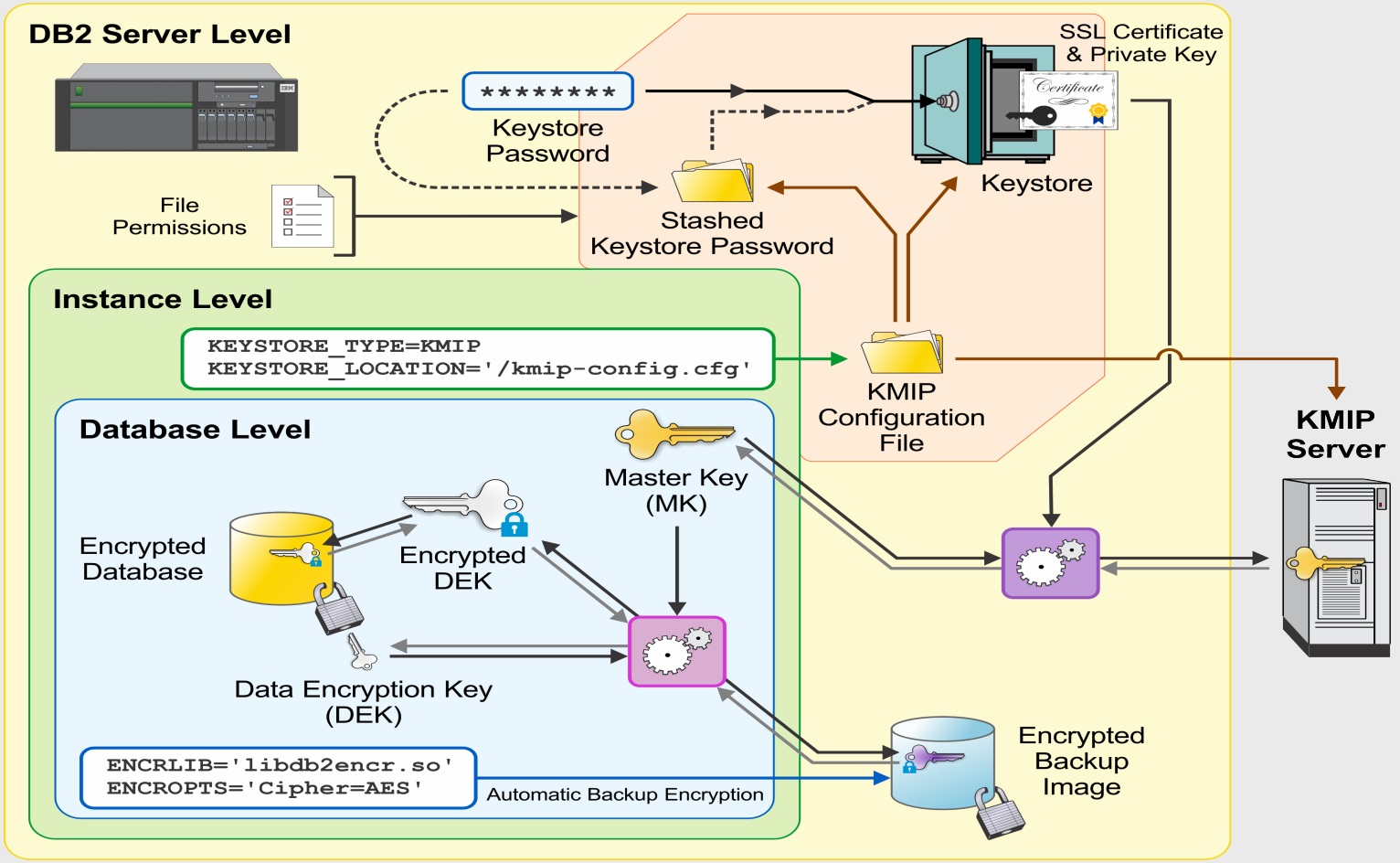


Image source: http://www.ibmbigdatahub.com/blog/db2-release-doubles-down-data-protection

Encryption Solution Example: DB2 Native Encryption / HSM

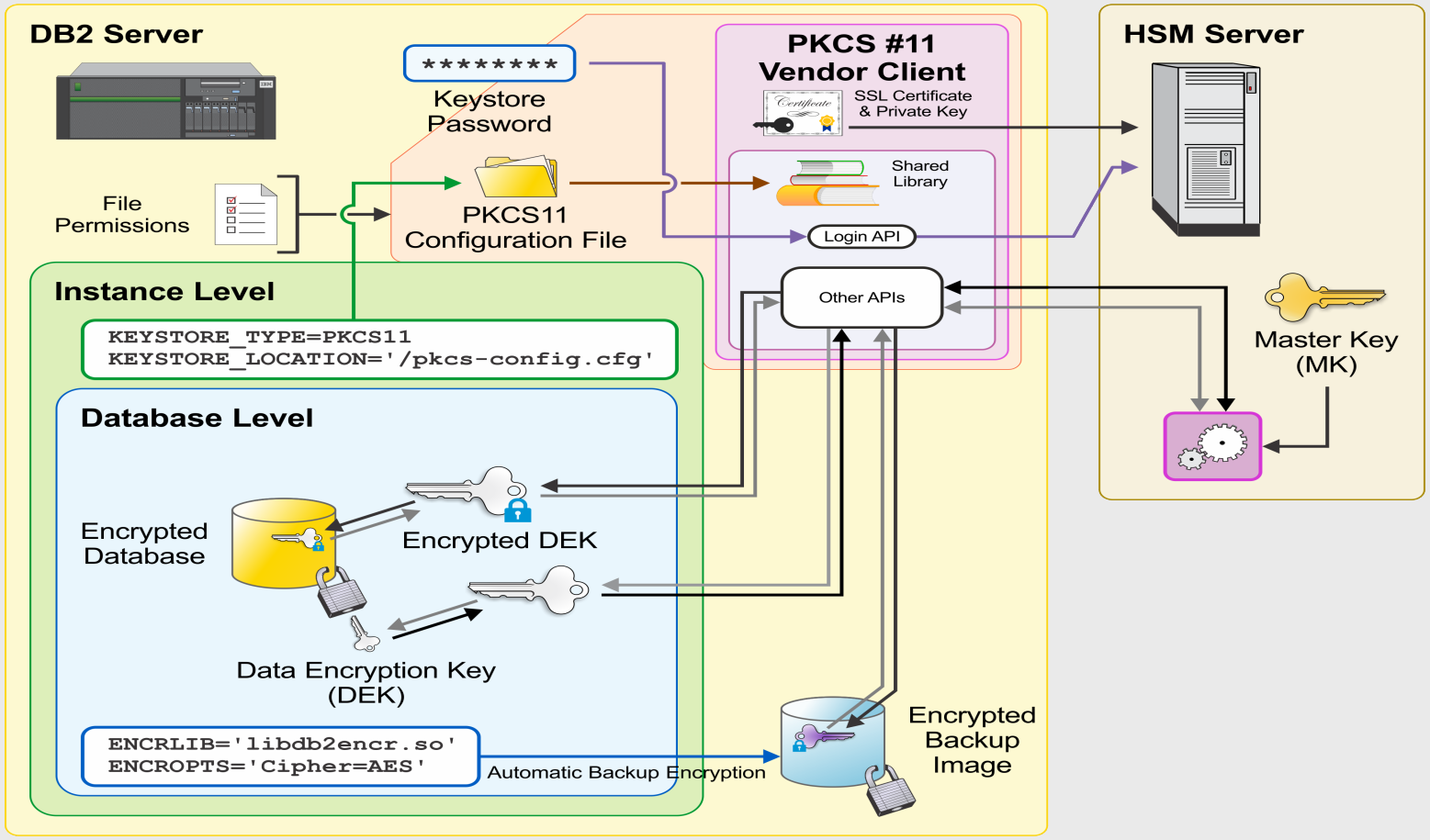
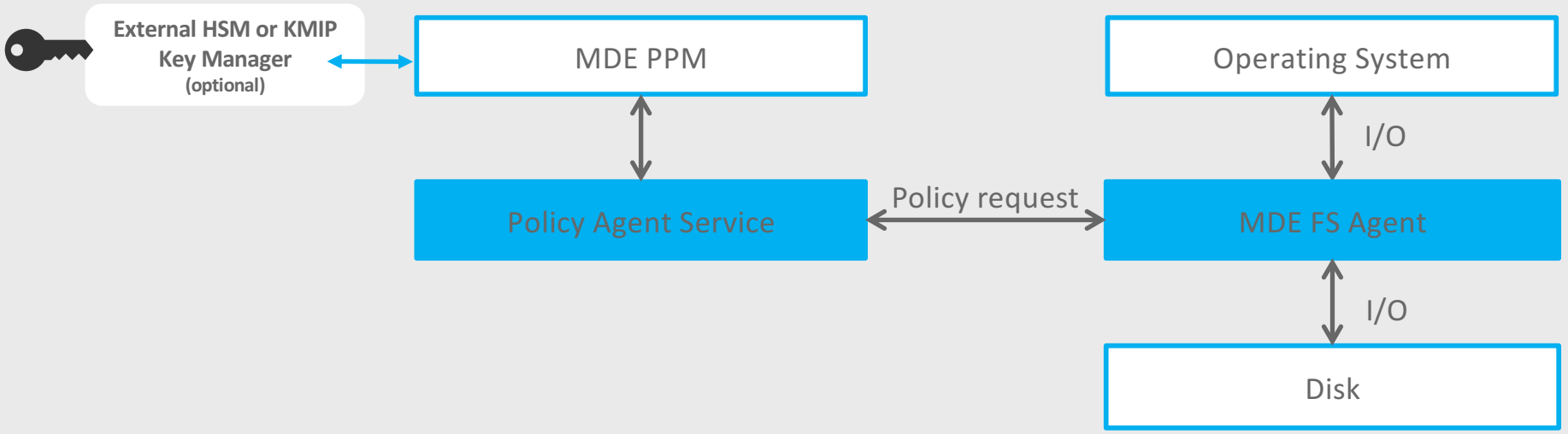
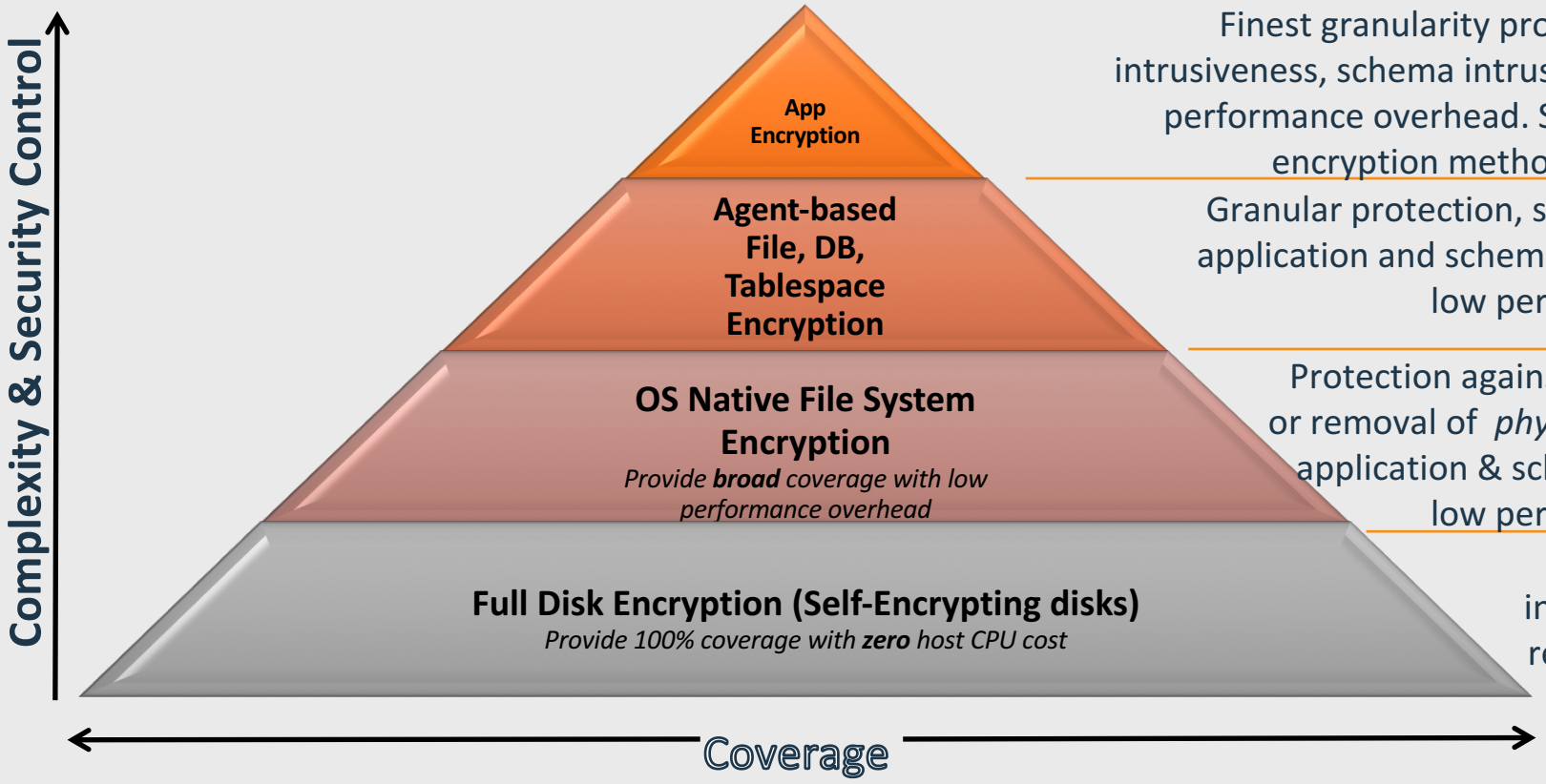


Image source: http://www.ibmbigdatahub.com/blog/db2-release-doubles-down-data-protection

Encryption Solution Example: Multi-Cloud Data Encryption (MDE)



Navigating the Encryption Solutions Landscape



Finest granularity protection, application intrusiveness, schema intrusiveness, and higher performance overhead. Suitable when other encryption methods are not available

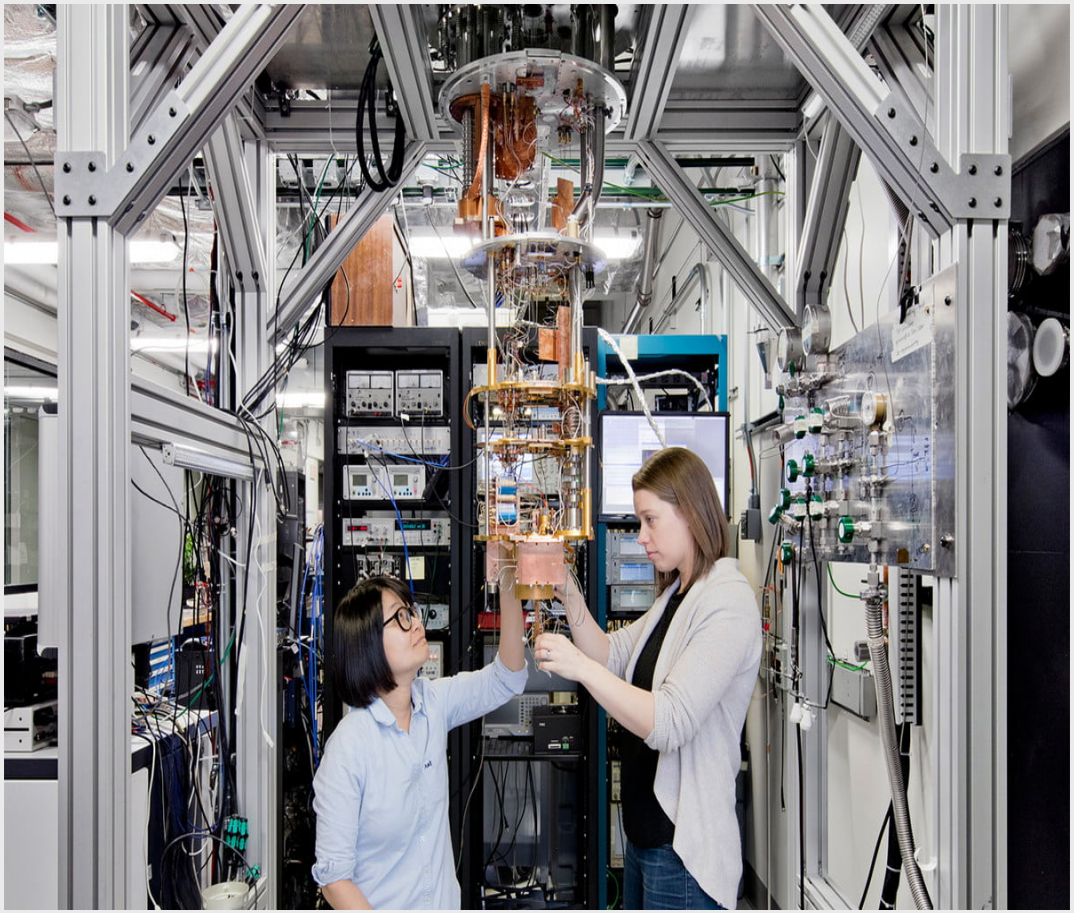
Granular protection, separation of duties, application and schema transparency, and low performance overhead

Protection against intrusion, tamper or removal of *physical* infrastructure, application & schema transparency, low performance overhead

Protection against intrusion, tamper or removal of *physical* infrastructure

Quantum Computers

- Exploit quantum mechanics to process information
- Use **qubits** which can represent 0, 1, or both at the same time
- Compute much faster than classical computers
- Large-scale quantum computers are still **decades** away



How Quantum Computers Will Affect Encryption

- Asymmetric encryption based on integer factoring and discrete logarithms will need to be replaced
- Symmetric algorithms will need double the key sizes

Encryption Algorithm	Key Size	Security Level on Classical Computer	Security Level on Quantum Computer
RSA-1024	1024 bits	80 bits	0
RSA 2048	2048 bits	120 bits	0
ECC 256	256 bits	128 bits	0
ECC 384	384 bits	192 bits	0
AES 128	128 bits	128 bits	**64 bits**
AES 256	256 bits	256 bits	**128 bits**

Quantum Algorithms

Shor's algorithm

Exponential improvement in brute-force attacks on asymmetric encryption schemes like RSA, ECC, ElGamel, DH

Grover's algorithm

Quadratic improvement in brute-force attacks on symmetric encryption schemes like AES

Example Implication

- Secure communication protocols: SSL, TLS, HTTPS, SSH

- **Shor's algorithm** running on a large-scale quantum computer may allow an attacker to:
  - **Derive the session key agreed to using RSA** during protocol handshake
  - Use the session key derived to decrypt the data exchanged later on

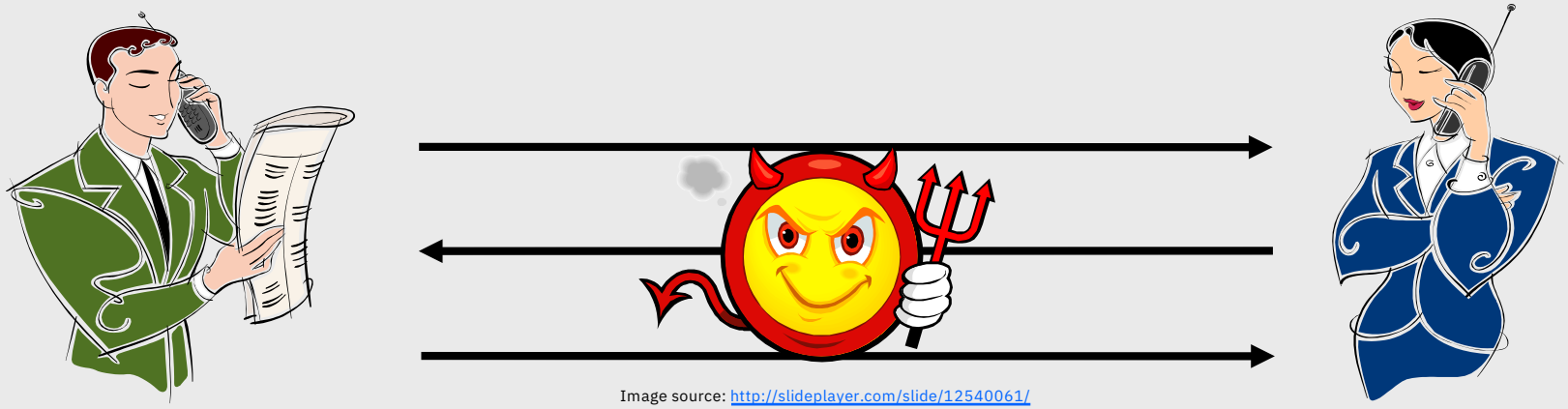


Image source: http://slideplayer.com/slide/12540061/

Example Implication (cont.)

- Secure communication protocols: SSL, TLS, HTTPS, SSH
- **Store copies of today's communications** and **decrypt them later** on when large-scale quantum computers become available

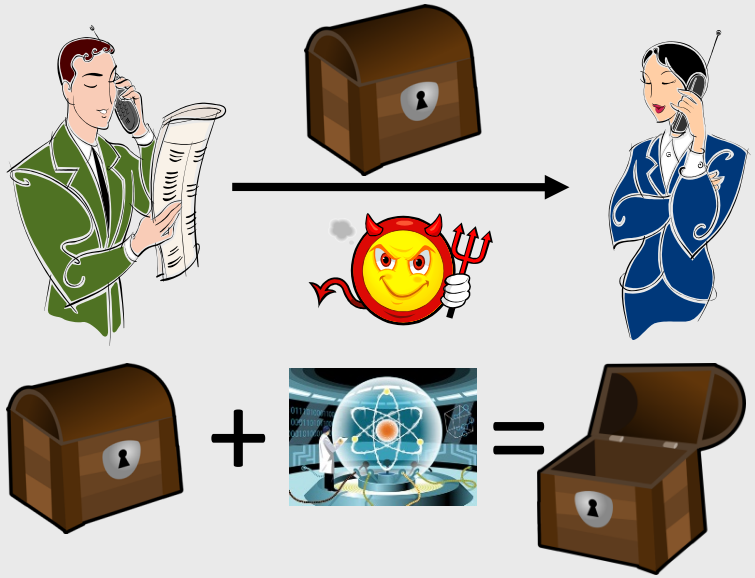


Image source: http://slideplayer.com/slide/12540061/

Post-Quantum Cryptography (PQC)

- Refers to new asymmetric algorithms which are resistant to attacks by quantum computers
- Based on a different set of mathematical problems such as Lattices
- **NIST call for proposals** around PQC closed in 4Q2017
  - > 80 proposals received from 25 countries / 5 continents
  - 1st NIST PQC Standardization Conference in April 2018
- **NIST will update guidance** when PQC standards are available

Next Steps?

- Understand where and how encryption is being used in your organization

- **For symmetric algorithms (AES, 3DES)**
  - Plan to transition to longer key sizes
    - A good practice regardless of quantum computing

- **For asymmetric algorithms (RSA, ECC)**
  - Minimize use of today's asymmetric algorithms (use symmetric instead)
  - Work with your encryption solution provider to adopt new algorithms will be available
  - Plan to transition accordingly

- **For Hash Algorithms (SHA-2, SHA-3)**
  - Longer output is required

NIST References:

Post-Quantum Cryptography:
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

NISTIR 8105 – Report on Post-Quantum Cryptography:
https://csrc.nist.gov/publications/detail/nistir/8105/final

Notices and disclaimers

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.** The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

Have breakfast with us on Wednesday, learn about encryption!

WHO: Any IBM client interested in learning about data encryption or using it today

WHAT: IBM Multi-Cloud Data Encryption client breakfast, hosted by SecurityFirst

WHEN: 7:15 - 8:15 AM PST, Wednesday, March 21st

WHERE: Four Seasons Hotel Las Vegas, Mesquite Room

HOW: Register at ibm.biz/encryption

WHY: Learn about Multi-Cloud Data Encryption from experts, meet peers with similar interests, ask questions and share best practices

Note: Seating is limited to the first 50 registrants

Thank you

Walid Rjaibi
CTO & DE for Data Security
IBM
—
wrjaibi@ca.ibm.com
+1-905-413-3410
ibm.com