Hewlett Packard Enterprise

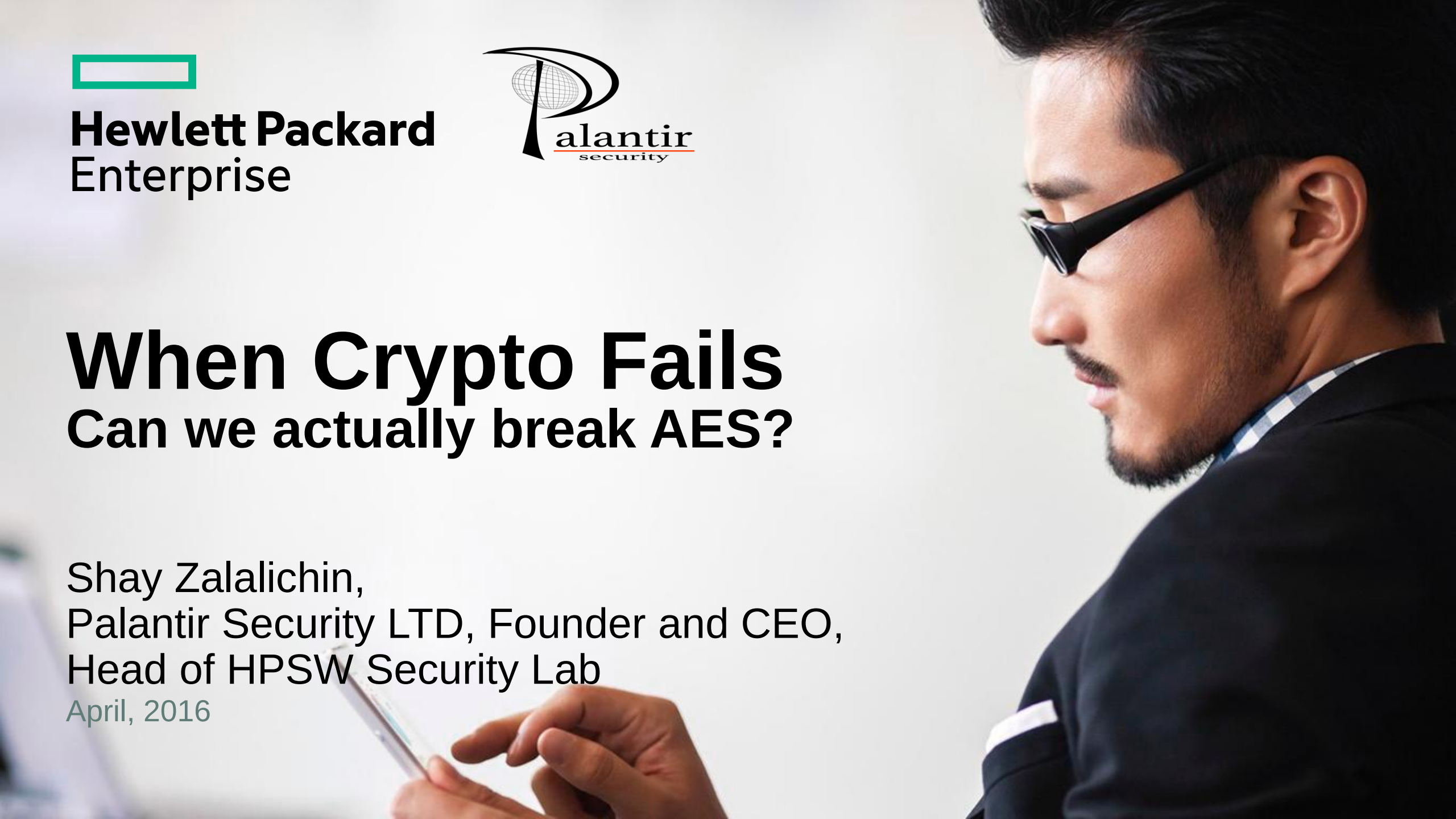
Palantir security

When Crypto Fails

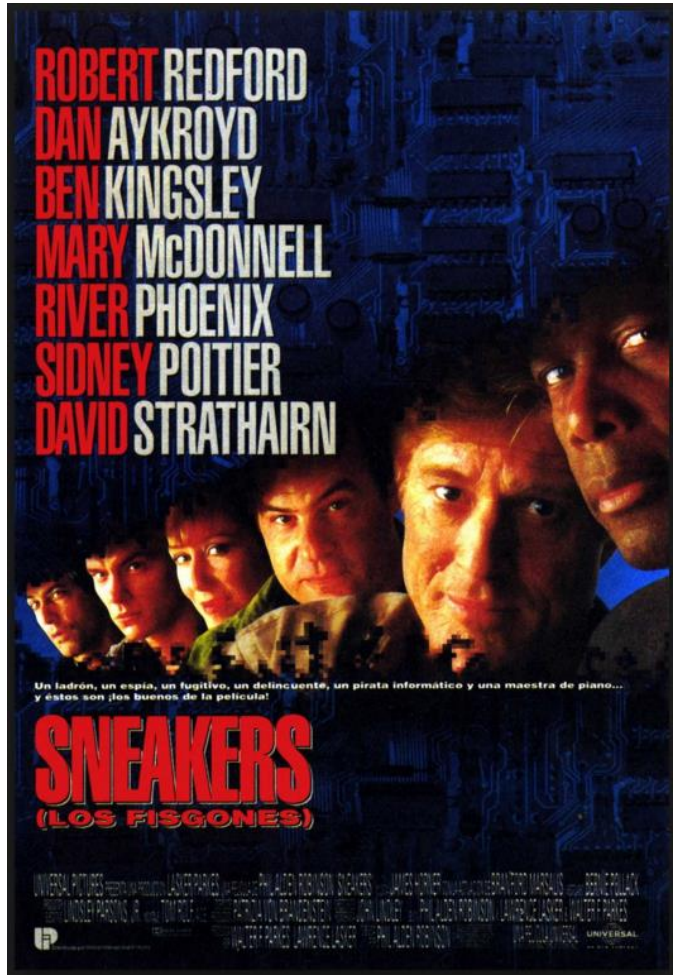
Can we actually break AES?

Shay Zalalichin,
Palantir Security LTD, Founder and CEO,
Head of HPSW Security Lab

April, 2016



When Crypto Fails



Regulation vs. Security

PCI Security Standards Council

PCI DSS Requirements	Testing Procedures	Guidance
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	**3.4.a** Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: • One-way hashes based on strong cryptography, • Tr • In st • Si pr **3.4.b** E reposit not sto **3.4.c** E back-u **3.4.d** E rendered unreadable or removed from the logs. **3.4.e** If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted using a matching one-time pad and key. The intent of strong cryptography (as defined in

Strong Cryptography	Cryptography based on industry-tested and accepted algorithms, along with strong key lengths (minimum 112-bits of effective key strength) and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way"). At the time of publication, examples of industry-tested and accepted standards and algorithms for minimum encryption strength include AES (128 bits and higher), TDES (minimum triple-length keys), RSA (2048 bits and higher), ECC (160 bits and higher), and ElGamal (2048 bits and higher). See NIST Special Publication 800-57 Part 1 (http://csrc.nist.gov/publications/) for more guidance on cryptographic key strengths and algorithms.

The Security Myth

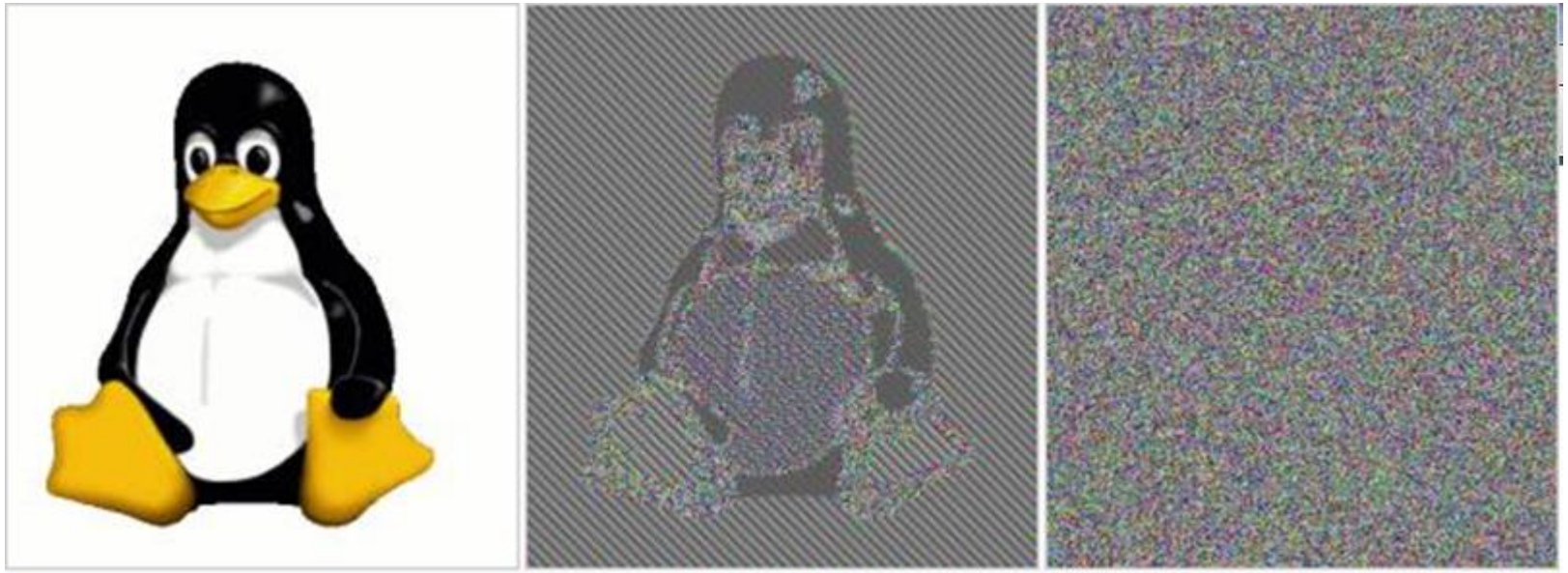
“AES/CBC/PKCS7 and Decent Key Management will do the job”

Problem #1 – Cryptography is Complex

Short Survey (Vote Yes or No)

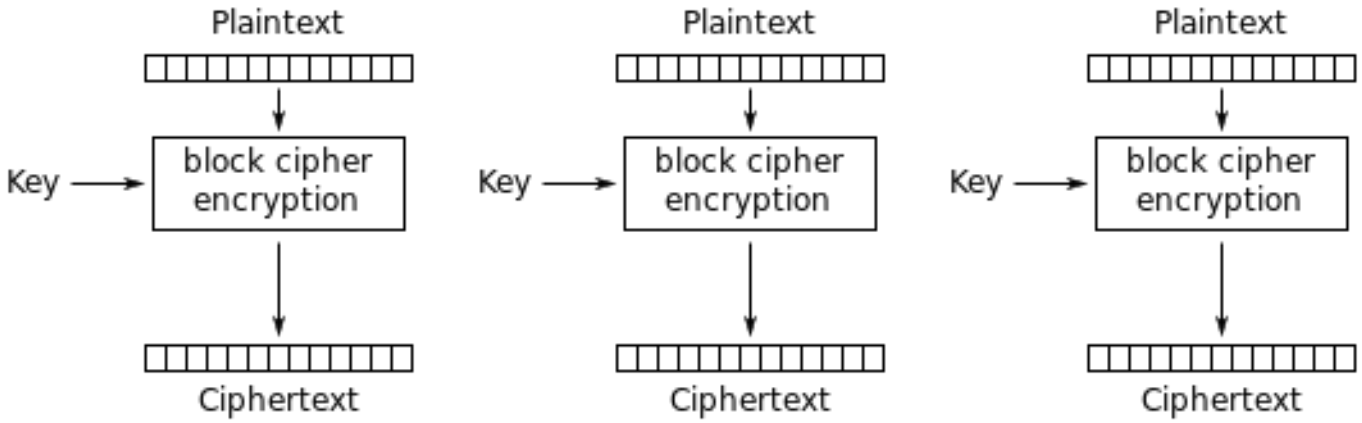
- Mode of Operation
- ECB
- CBC
- CTR
- OFB
- CFB
- GCM
- CCM
- AE/AEAD

ECB vs. CBC



Original image | Encrypted using ECB mode | Encrypted using CBC mode

Why ECB is Bad



Electronic Codebook (ECB) mode encryption

Spot the Problem

https://docs.oracle.com/javase/8/docs/api/javax/crypto/Cipher.html

OVERVIEW PACKAGE CLASS USE TREE DEPRECATED INDEX HELP

Java™ Platform Standard Ed. 8

PREV CLASS NEXT CLASS FRAMES NO FRAMES ALL CLASSES

SUMMARY: NESTED | FIELD | CONSTR | METHOD DETAIL: FIELD | CONSTR | METHOD

compact1, compact2, compact3

javax.crypto

Class Cipher

java.lang.Object
    javax.crypto.Cipher

Direct Known Subclasses:

NullCipher

```
public class Cipher
extends Object
```

This class provides the functionality of a cryptographic cipher for encryption and decryption. It forms the core of the Java Cryptographic Extension (JCE) framework.

In order to create a Cipher object, the application calls the Cipher's `getInstance` method, and passes the name of the requested *transformation* to it. Optionally, the name of a provider may be specified.

A *transformation* is a string that describes the operation (or set of operations) to be performed on the given input, to produce some output. A transformation always includes the name of a cryptographic algorithm (e.g., *DES*), and may be followed by a feedback mode and padding scheme.

A transformation is of the form:

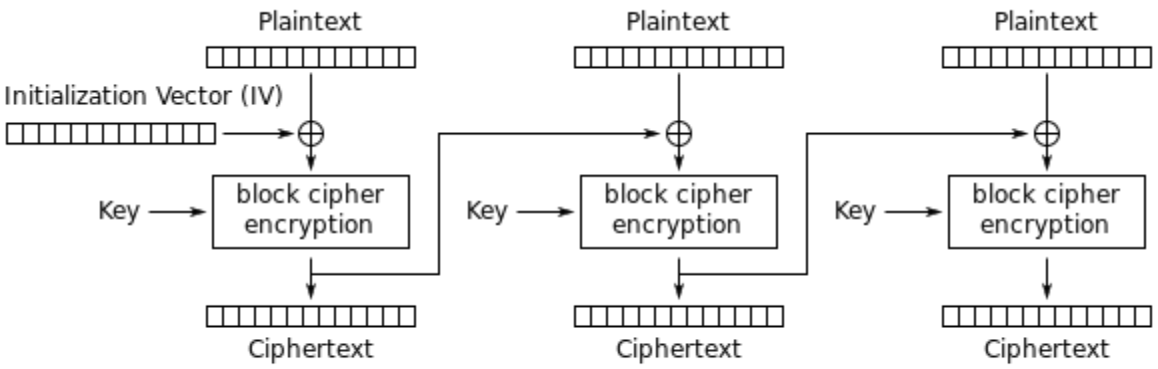
- "*algorithm/mode/padding*" or
- "*algorithm*"

(in the latter case, provider-specific default values for the mode and padding scheme are used). For example, the following is a valid transformation:

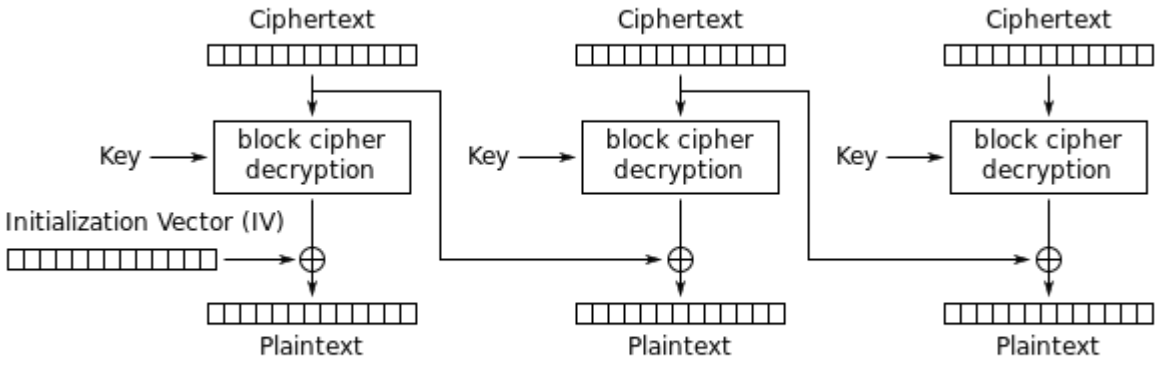
```
Cipher c = Cipher.getInstance("DES/CBC/PKCS5Padding");
```

Using modes such as `CFB` and `OFB`, block ciphers can encrypt data in units smaller than the cipher's actual block size. When requesting such a mode, you may optionally specify the number of bits to be processed at a time by appending this number to the mode name as shown in the "`DES/CFB8/NoPadding`" and "`DES/OFB32/PKCS5Padding`" transformations. If no such number is specified, a provider-specific default is used. (For example, the SunJCE provider uses a default of 64 bits for DES.) Thus, block ciphers can be turned into byte-oriented stream ciphers by using an 8 bit mode such as CFB8 or OFB8.

How CBC Works



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

So, is CBC Secure?

A. Yes

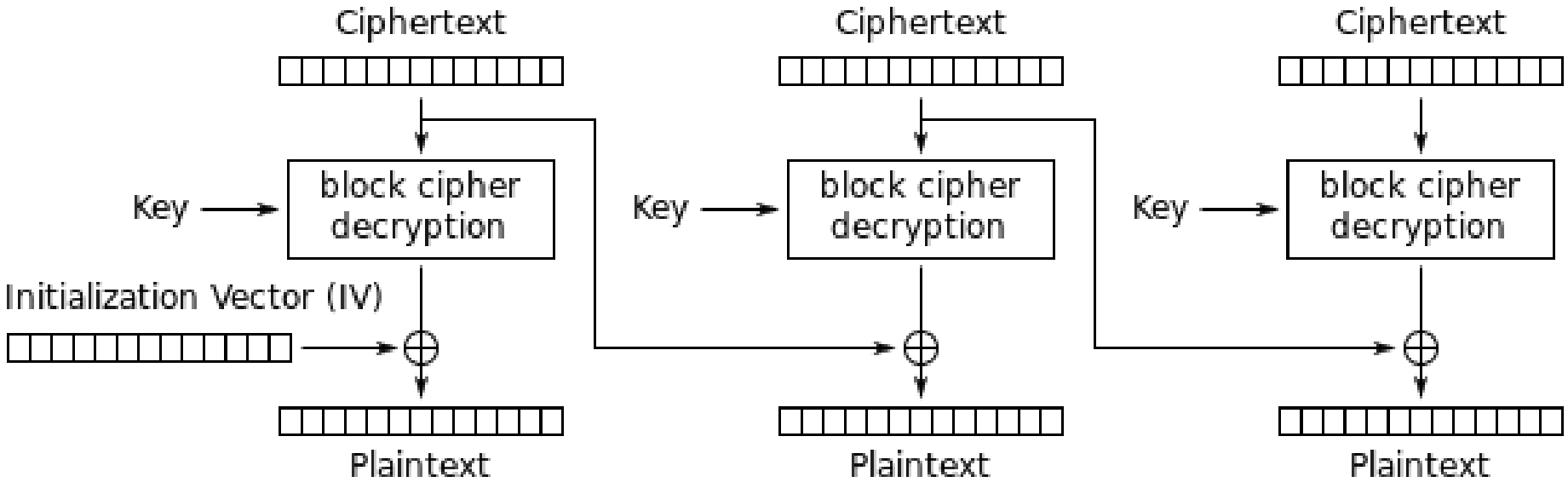
B. No

C. It Depends

D. Other

So, is CBC Secure?

Let’s Have a Closer Look on CBC



Cipher Block Chaining (CBC) mode decryption

So, Is CBC Secure??

CPA Secure

Vs.

CCA Secure

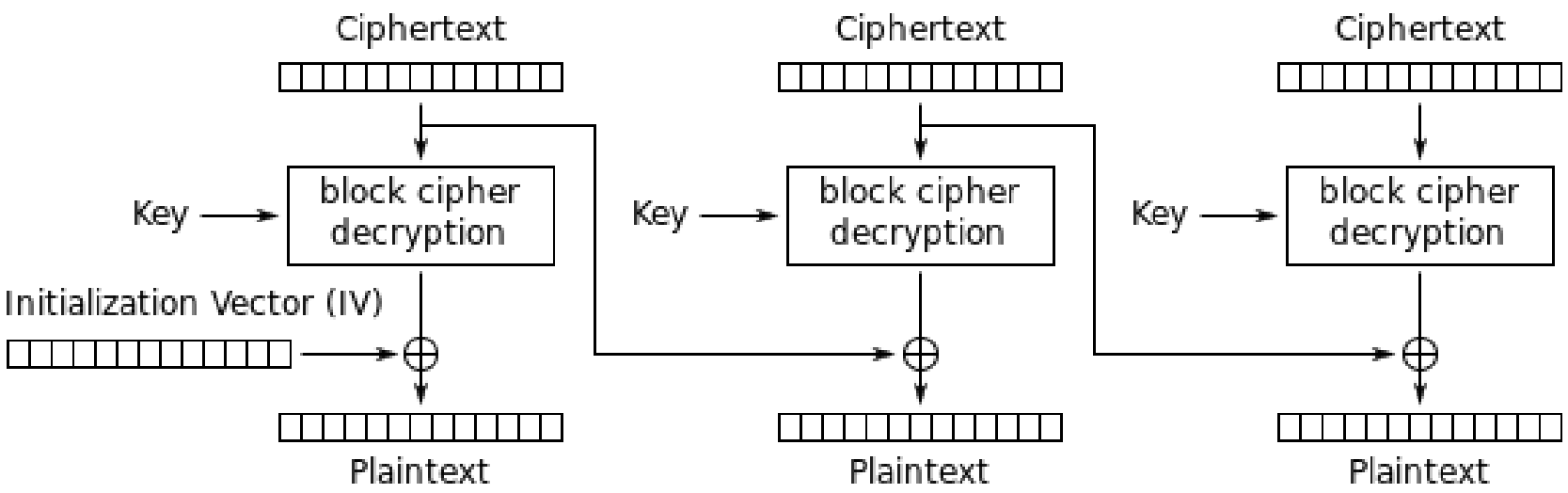
Quick XOR Recap

Exclusive-OR gate

A	B	Output
0	0	0
0	1	1
1	0	1
1	1	0

Let’s Have (again) a Closer Look on CBC

Spot the problem …



Cipher Block Chaining (CBC) mode decryption

Demo Time

Time For Conclusions

- Cryptography is a complex subject
- Never assume that strong crypto is the solution to all the world's problems
- Know what are you trying to solve
- Know what you are doing
- Pay attention to the little details

- Use Authenticated Encryption whenever Integrity is needed (e.g. GCM)
- Never, but never try to re-invent the wheel

Hewlett Packard
Enterprise

Thank you

Questions?