FLIPSIDE
smart content provider

Modos de Operação de Cifras de Bloco

GTS14

Anderson Ramos

FLIPSIDE
smart content provider

Afinal, o que são os modos de sei lá o quê?

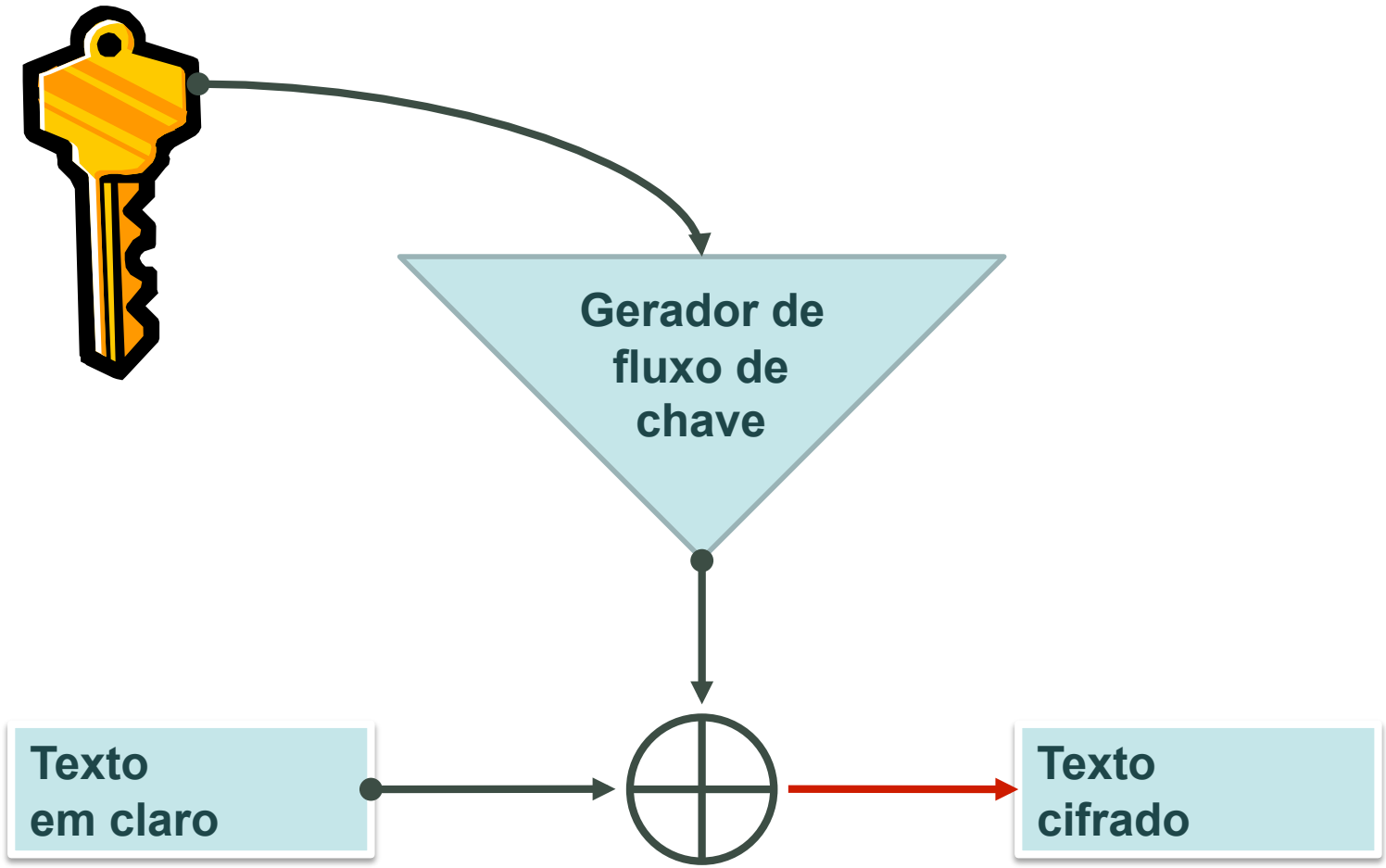
AV. DAS NAÇÕES UNIDAS 12.551 / 9° ANDAR
CEP 04578-000 / SÃO PAULO / SP / BRASIL
T +55 (11) 3443-7740
F +55 (11) 3443-7474
WWW.FLIPSIDE-SCP.COM
CONTATO@FLIPSIDE-SCP.COM

FLIPSIDE
smart content provider

"Cryptography has often been used to protect the wrong things, or used to protect them in the wrong way" – Ross Anderson

AV. DAS NAÇÕES UNIDAS 12.551 / 9° ANDAR
CEP 04578-000 / SÃO PAULO / SP / BRASIL
T +55 (11) 3443-7740
F +55 (11) 3443-7474
WWW.FLIPSIDE-SCP.COM
CONTATO@FLIPSIDE-SCP.COM

Cifras de Fluxo



FLIPSIDE
smart content provider

Legenda

IV — **Initialization Vector**

PTB — **Plain Text Block**

CTB — **Cipher Text Block**

Cipher Text Block

Em claro

Cifrado

Remoção de padrões

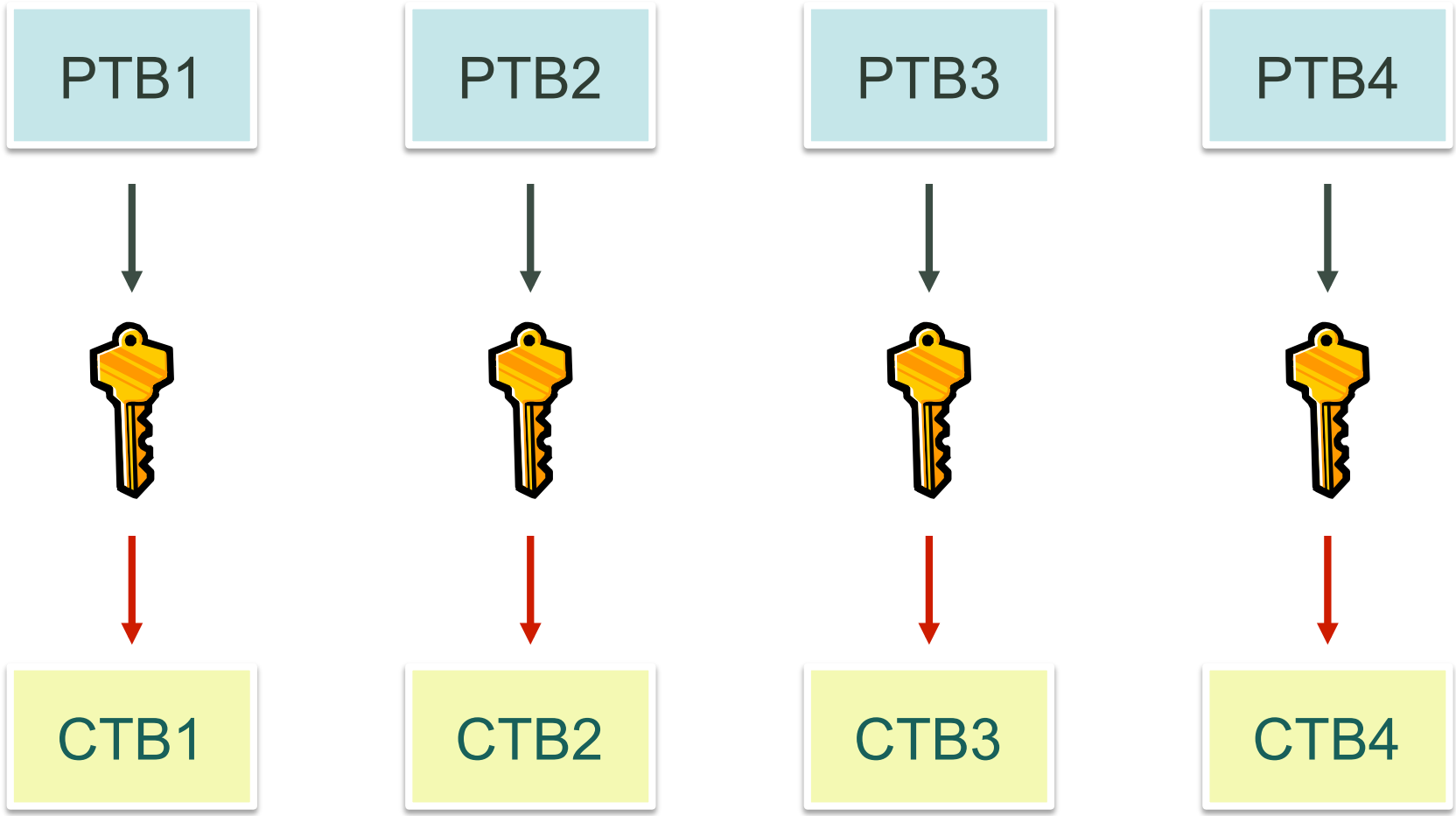
Aleatório

XOR

AV. DAS NAÇÕES UNIDAS 12.551 / 9° ANDAR
CEP 04578-000 / SÃO PAULO / SP / BRASIL
T +55 (11) 3443-7740
F +55 (11) 3443-7474
WWW.FLIPSIDE-SCP.COM
CONTATO@FLIPSIDE-SCP.COM

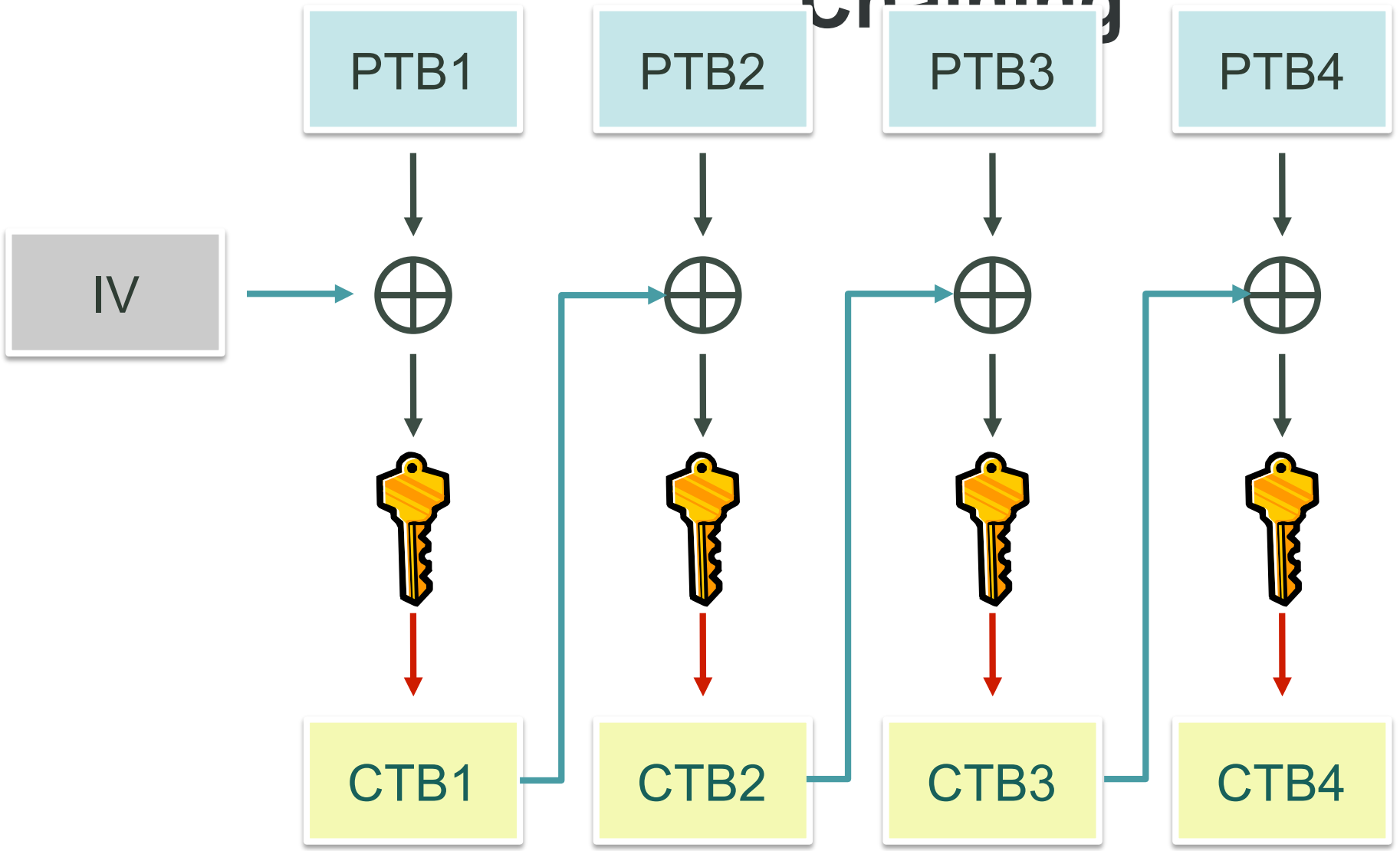
FLIPSIDE
smart content provider

ECB – Electronic Code Book



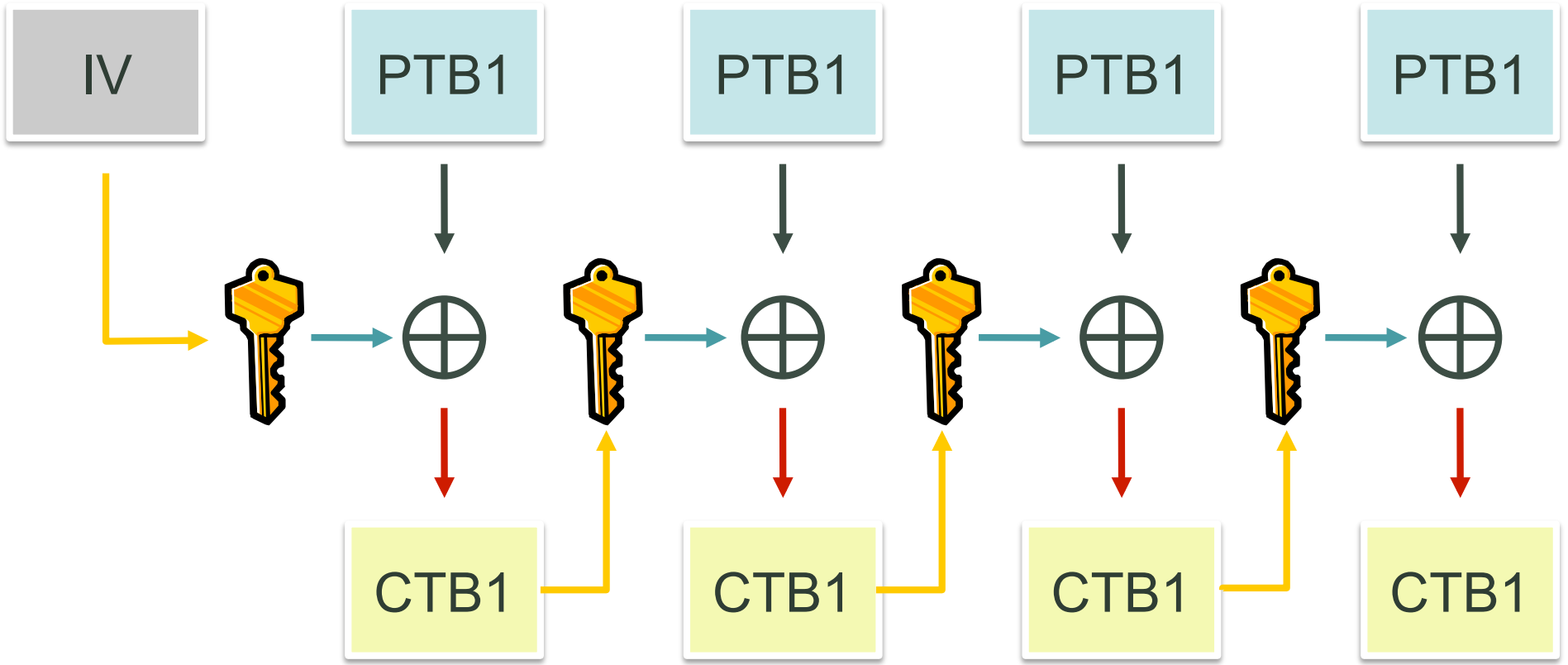
FLIPSIDE
smart content provider

CBC– Cipher Block Chaining



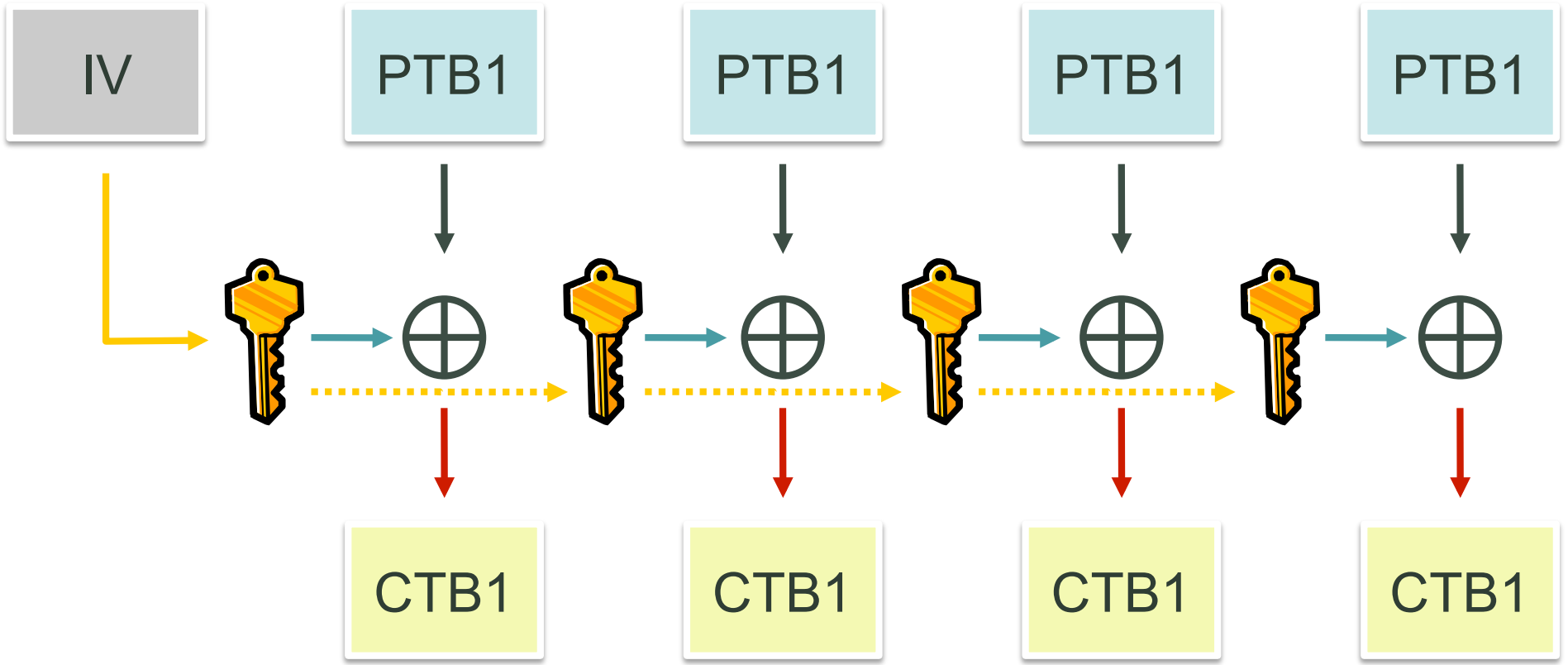
FLIPSIDE
smart content provider

CFB– Cipher Feed Back



FLIPSIDE
smart content provider

OFB– Output Feed Back



Perguntas?

WWW.FLIPSIDE-SCP.COM

Anderson Ramos

aramos@flipside-scp.com.br
Twitter – aramosorg
Blog – aramos.org
www.linkedin.com/in/aramos