

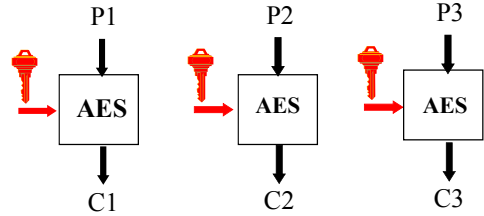
Modes of Operation of a Block Cipher

Prof. Bart Preneel
COSIC, KU Leuven

Bart.Preneel(at)esat.kuleuven.be
<http://homes.esat.kuleuven.be/~preneel>
December 2014


1

How NOT to use a block cipher: ECB mode (Electronic Code Book)



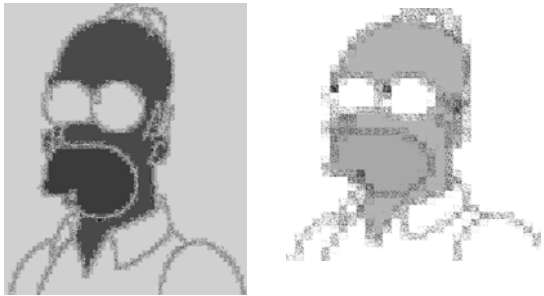
2

An example plaintext



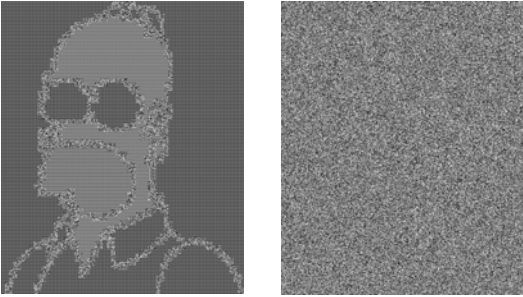
3

Encrypted with substitution and transposition cipher



4

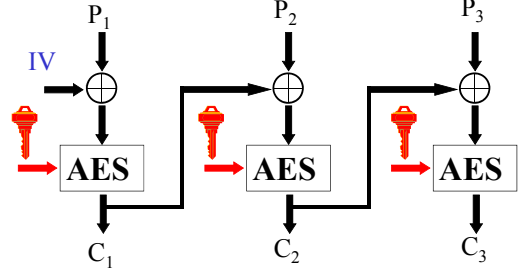
Encrypted with AES in ECB and CBC mode



5

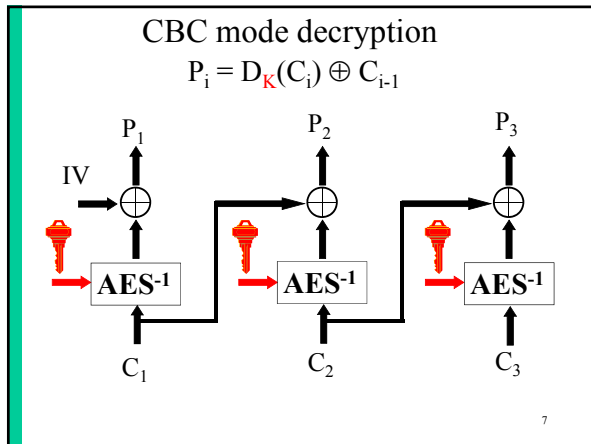
How to use a block cipher: CBC mode

Cipher Block Chaining $C_i = E_k(P_i \oplus C_{i-1})$

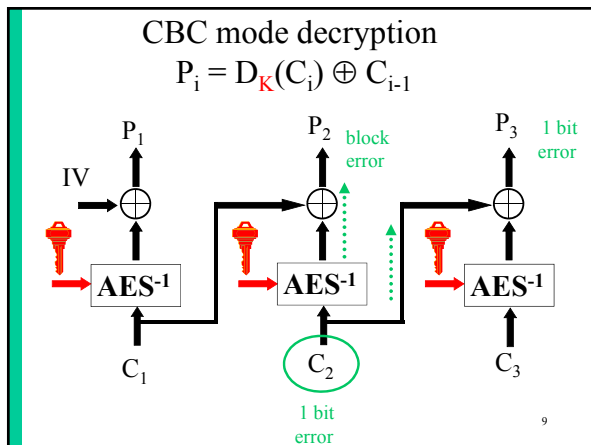


need random and secret IV

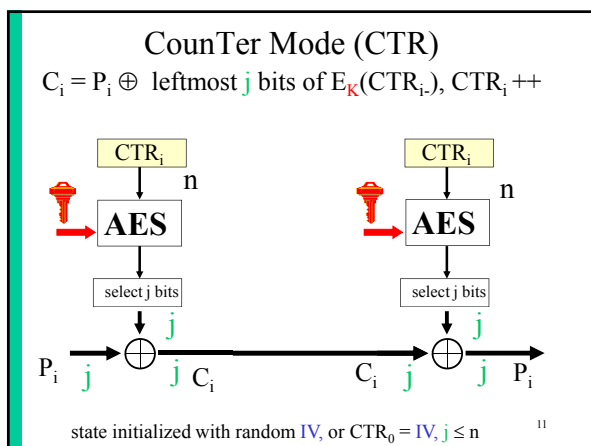
6



- CBC properties**
- propagation from left to right
 - random and secret IV: hides repetitions in the beginning of the plaintext
 - encryption only from left to right, but decryption with random access
 - need integral number of blocks (n bits)
 - decryption with limited error propagation
- 8



- CBC is “secure” against chosen plaintext attack (informal)**
- [Bellare et al. 97]
- If AES is a “secure” n-bit block cipher, then AES in CBC mode with a random and secret IV is an encryption algorithm “secure” against chosen plaintext attacks provided that you encrypt at most r blocks with $r \ll 2^{n/2}$
- 10



- CTR: properties**
- similar properties as OFB
 - but random access on decryption
 - but better suited for hardware:
 - parallelism: one can process multiple counter values at the same time
 - pipelining: no need to know the ciphertext block corresponding to the current plaintext block to start processing the next plaintext block
 - risk: what if counters are (accidentally) reset to same value?
- 12

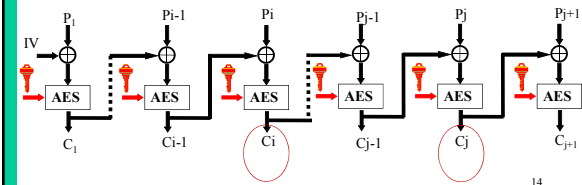
Overview modes: when to use

- ECB: never
- CBC: current workhorse – to be replaced by authenticated encryption (see later)
- CTR: no error propagation (e.g. wireless); pipelining (high speed hardware or use of Intel instruction)

13

Limits of CBC security

- matching lower bound:
 - collision $C_i = C_j$ implies $C_{i-1} \oplus P_i = C_{j-1} \oplus P_j$
 - collision expected after $r = 2^{n/2}$ blocks



14

The birthday paradox (1)

- Given a set with S elements
- Choose r elements at random (with replacements) with $r \ll S$
- The probability p that there are at least 2 equal elements (a collision) is $1 - \exp(-r(r-1)/2S)$
- S large, $r = \sqrt{S}$, $p = 0.39$
- $S = 365$, $r = 23$, $p = 0.50$

15

The birthday paradox (2) – no proof

- Given a set with S elements, in which we choose r elements at random (with replacements) with $r \ll S$
- The number of collisions follows a Poisson distribution with $\lambda = r(r-1)/2S$
 - The expected number of collisions is equal to λ
 - The probability to have c collision is $e^{-\lambda} \lambda^c / c!$

16

The birthday paradox: CBC (3)

- the ciphertext blocks C_i are random n -bit strings or $S = 2^n$
- if we collect $r = \sqrt{2^n} = 2^{n/2}$ ciphertext blocks, we will have a high probability that there exist two identical ciphertext blocks, that is, there exist indices i and j such that $C_i = C_j$
- this leaks information on the plaintext (see above)

17

The birthday paradox: CBC (4)

- for DES, $n = 64$: leakage after 2^{32} 64-bit blocks or 32 Gbyte
- for AES, $n = 128$: leakage only after 2^{64} 64-bit locks
- Example: DES with an encryption speed of 1 Gbit/s,
 - one expect the first collision after 4.5 minutes
 - After 19.5 hours, one has obtained 2^{40} ciphertext blocks; the expected number of collisions is then $(2^{40})^2 / 2^{65} = 2^{15}$
- Solution: change key quickly or use larger block length

18

CBC: insecurity against chosen ciphertext attack

- CBC is very easy to distinguish with **chosen ciphertext** attack:
 - decrypting $C \parallel C \parallel C$ yields $P' \parallel P \parallel P$

19

What if IV is constant/predictable

Repetition in P results in repetition in C:
⇒ information leakage

need random and secret IV²⁰

What if IV is predictable

If $C1 = C1'$ then $P1_{guess} = P1$

21

NIST's Modes of Operation for AES

- ECB/CBC/CFB/OFB + CTR (Dec 01)
- MAC algorithm: CMAC (May 05)
- Authenticated encryption:
 - CCM: CTR + CBC-MAC
 - GCM: Galois Counter Mode

Issues:

- associated data
- parallelizable
- on-line
- provable security

- IAPM
- XECB
- OCB
- CCM
- GCM
- (EAX)
- (CWC)

patented

22

Example: CCM: CTR + CBC-MAC

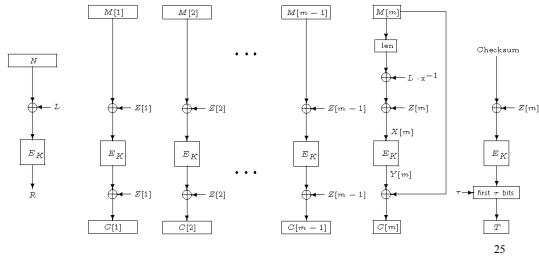
SN = packet sequence number (WEP "IV")

23

GCM = CTR + GMAC

24

OCB = masked ECB encryption +
encrypted simple checksum



25

Concrete recommendations

- AES-128 in CCM mode
 - CCM = CTR mode + CBC-MAC
 - change key after 2^{40} blocks
- Stream ciphers (better performance)
 - hardware: SNOW-3G, Trivium, Grain
 - software: HC-128, Salsa20

26

Exercises

1. A 64-bit block cipher is used in CBC mode with a speed of 2 Gigabit/s ($2 \cdot 10^9$ bits/s)
 - How long does it take before information starts to leak on the plaintext?
 - How many collisions do you expect after 1 hour?

27