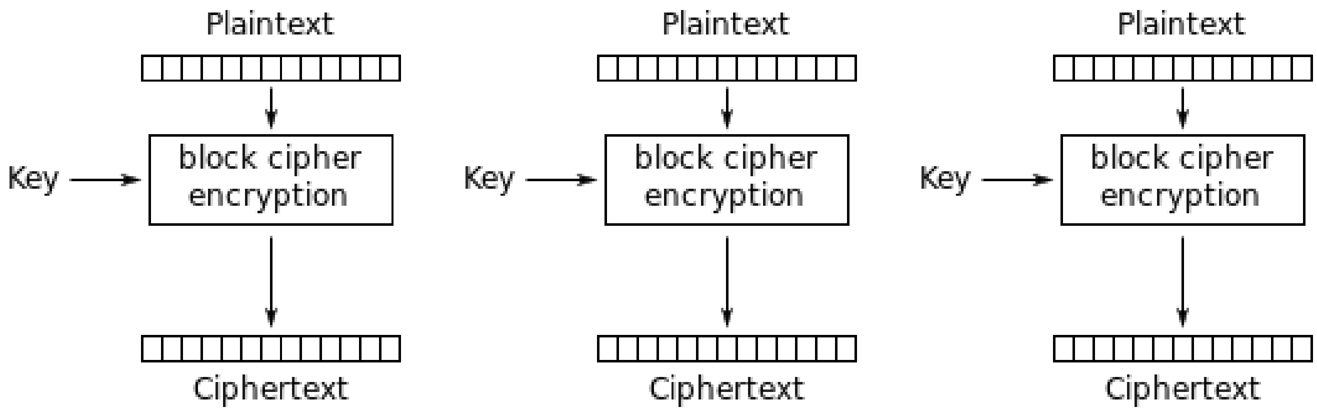
Cryptography

Lecture 6

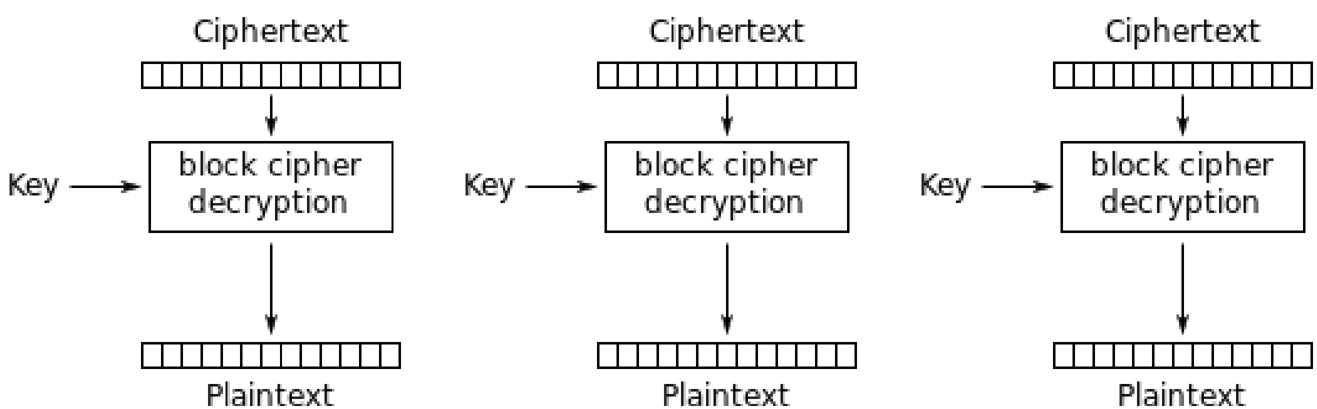
Vahid Amin-Ghafari
Vahidaming@ustc.edu.cn

Block cipher mode of operation

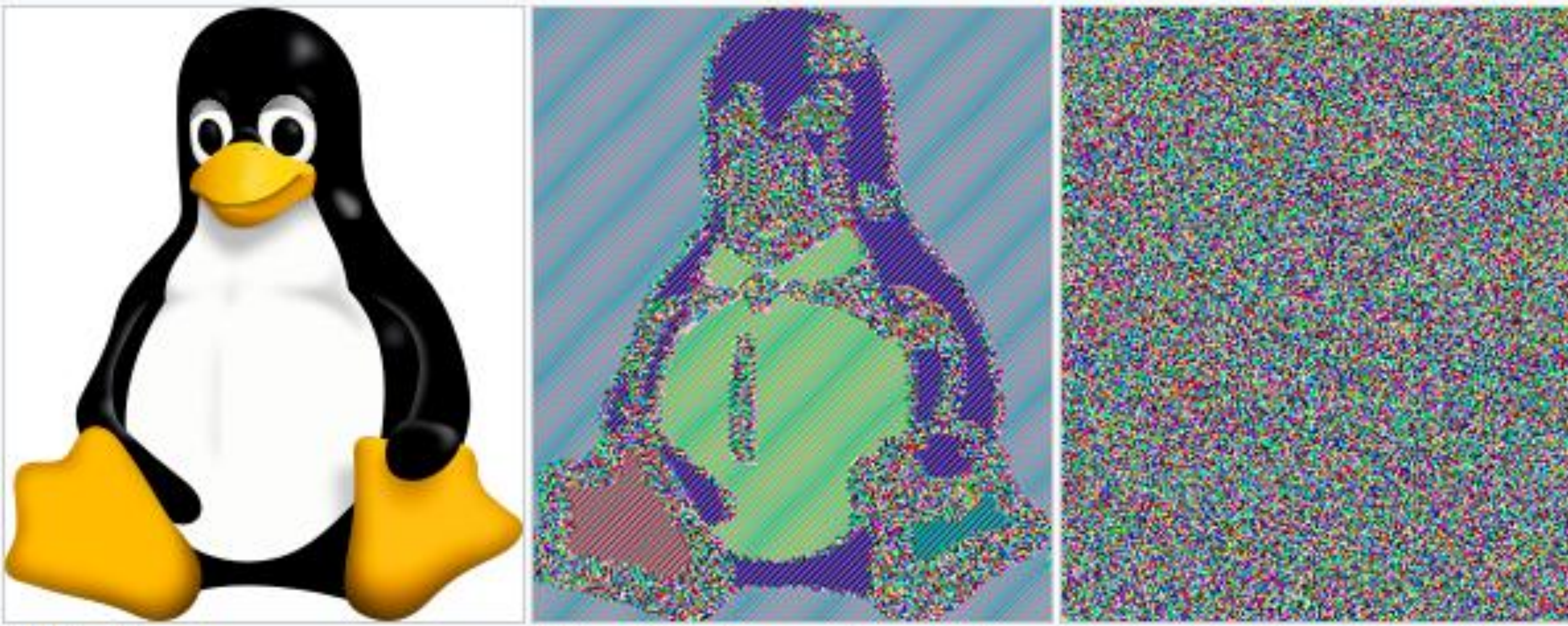
- Electronic Codebook (ECB):



Electronic Codebook (ECB) mode encryption



Block cipher mode of operation



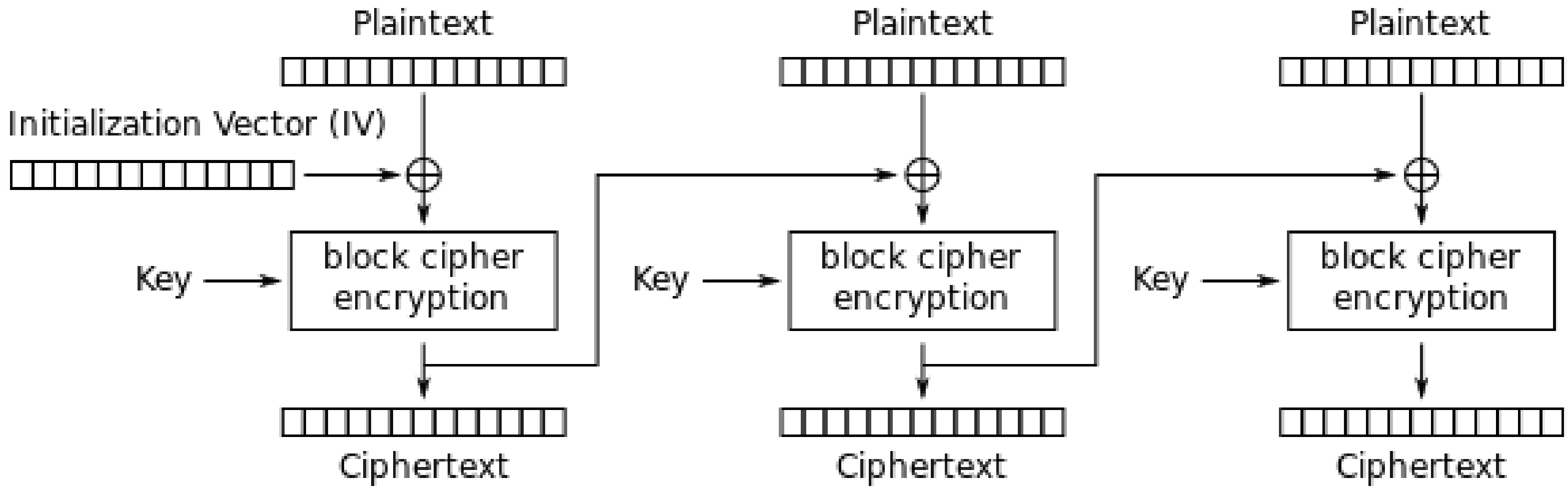
Original image

Using ECB allows patterns to be easily discerned

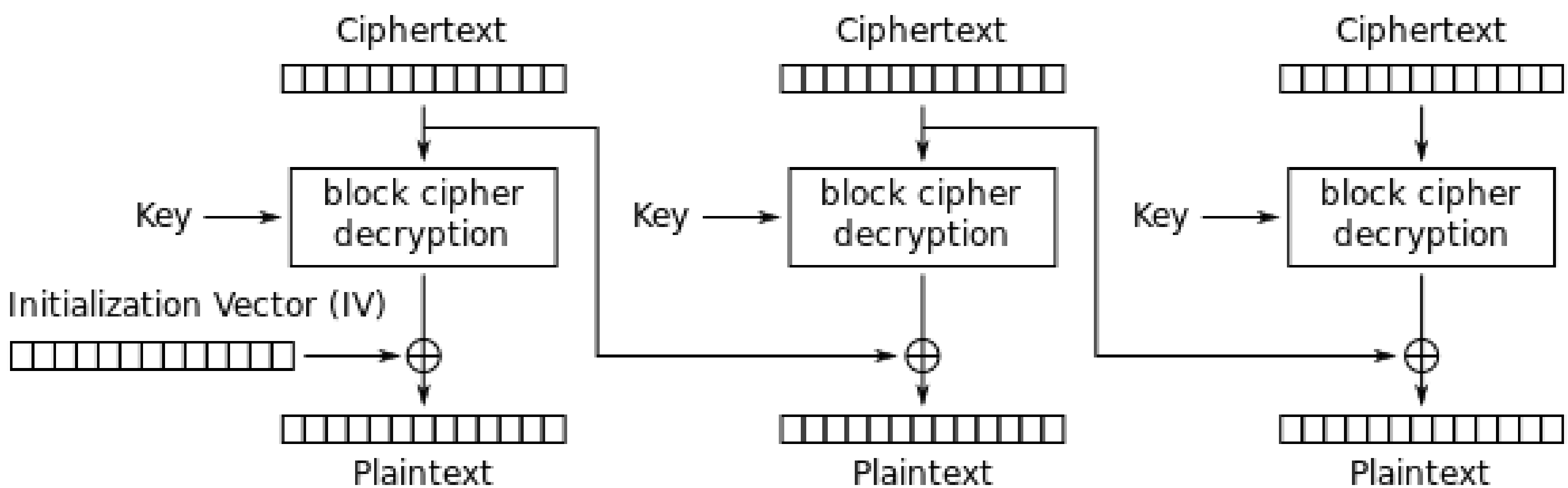
Modes other than ECB result in pseudo-randomness

Block cipher mode of operation

Cipher block Chaining (CBC)

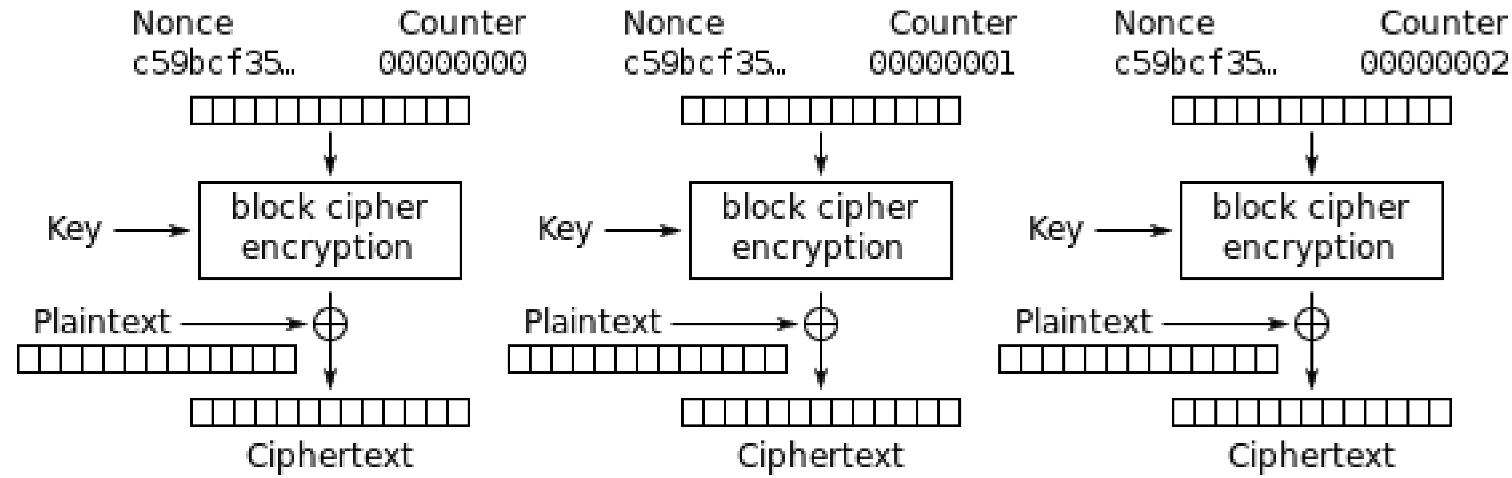


Cipher Block Chaining (CBC) mode encryption

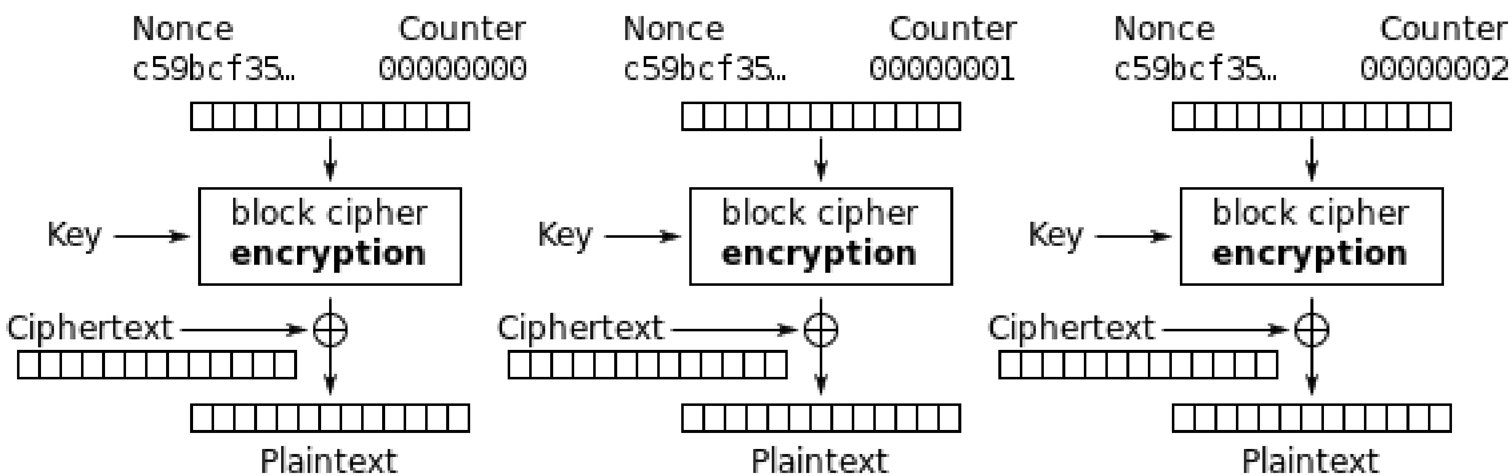


Block cipher mode of operation

Counter (CTR)



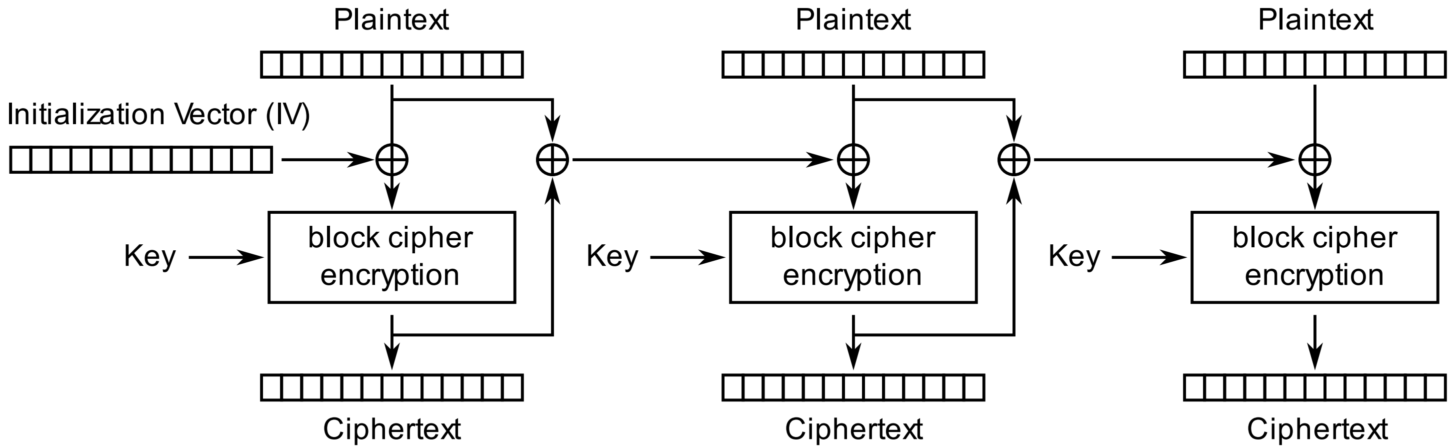
Counter (CTR) mode encryption



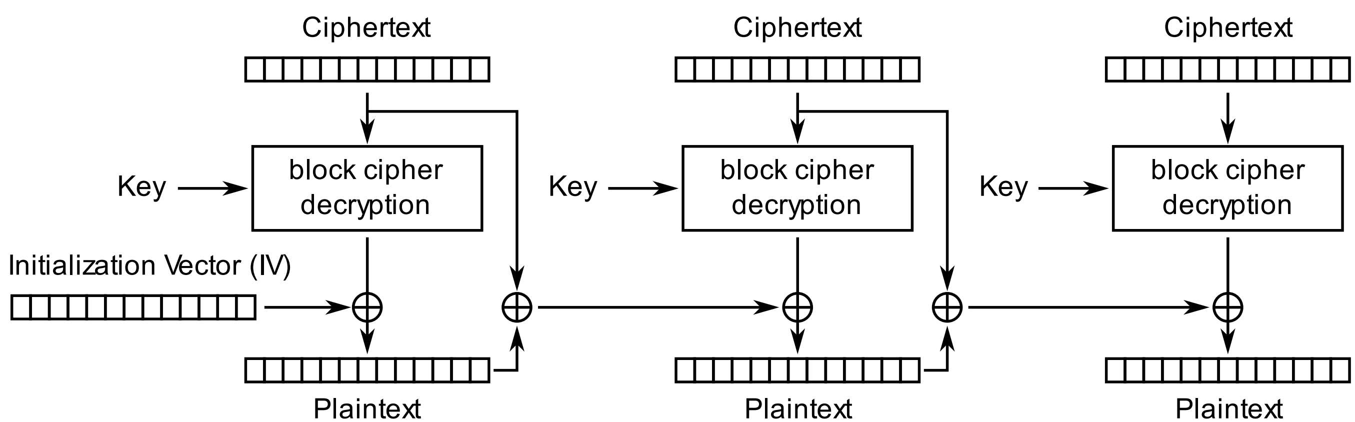
Counter (CTR) mode decryption

Block cipher mode of operation

Propagating cipher block chaining (PCBC)



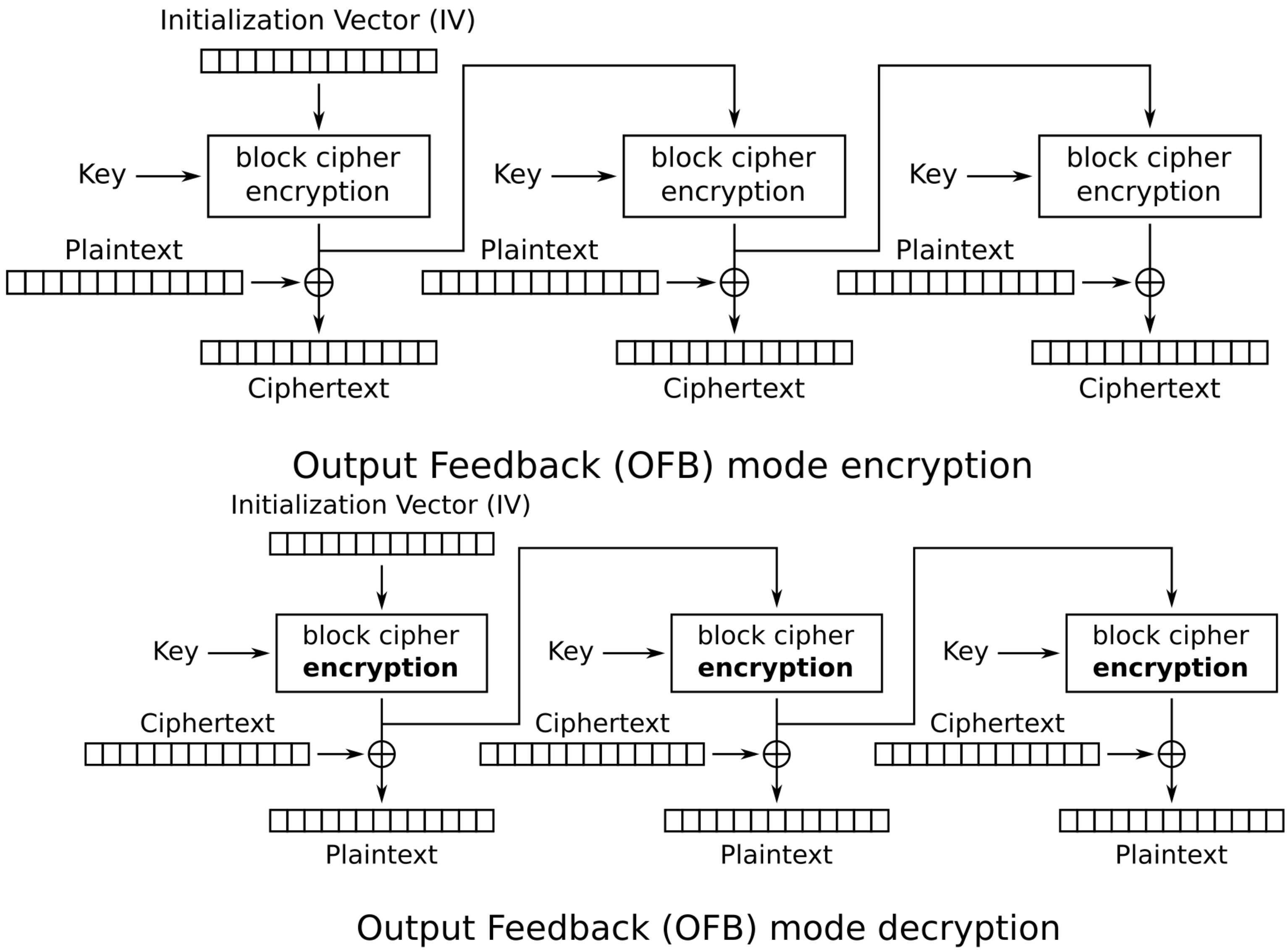
Propagating Cipher Block Chaining (PCBC) mode encryption



Propagating Cipher Block Chaining (PCBC) mode decryption

Block cipher mode of operation

Output feedback (OFB)



Bias

- Suppose that $X_1, X_2, ...$ are independent random variables taking on values from the set {0, 1}.
  - $\Pr[X_i = 0] = pi,\ \Pr[X_i = 1] = 1 - pi$
- $\Pr[Xi = 0, X_j = 0] = pi\, p_j$
- $\Pr[Xi = 0, X_j = 1] = pi(1 - p_j)$
  - $\Pr[X_i \oplus X_j = 0] = pi\, p_j + (1 - pi)(1 - p_j)$
- *The bias of X_i is defined to be the quantity:*

$$\epsilon_i = pi - {}^1\!/_2$$

Piling-up lemma

- LEMMA 4.1 (Piling-up lemma) Let $\epsilon_{i1,\ i2,\ \ldots,\ ik}$ denote the bias of the random variable:

  $X_{i1} \oplus \ldots . \oplus X_{ik}$,
- $\epsilon_{i1,\ i2,\ \ldots,\ ik} = 2^{k-2} \prod_{j=1}^{k} \epsilon_{ij}$
- Independent random variables
- PROOF (Homework)

Linear Approximations of S-boxes

- S-box $\pi_S : \{0, 1\}^m \rightarrow \{0, 1\}^n$.
- $X = (x_1, \ldots, x_m)$:
- x_i defines a random variable X_i taking on values 0 and 1 at random & independent. (ϵ_i =0)
- $Y = (y_1, \ldots, y_n)$:
- Not independent from each other or from the X_i
- $\Pr[X_1 = x_1, \ldots, X_m = x_m, Y_1 = y_1, \ldots, Y_n = y_n] =$
  0 if $(y_1, \ldots, yn) \neq \pi_S(x_1, \ldots, xm)$

Linear Approximations of S-boxes

- $\Pr[X_1 = x_1, \ldots, X_m = x_m, Y_1 = y_1, \ldots, Y_n = y_n] = 2^{-m1}$ if $(y_1, \ldots, yn) = \pi_S(x_1, \ldots, xm)$
- $\Pr[Y_1 = y_1, \ldots, Y_n = y_n | X_1 = x_1, \ldots, X_m = x_m] = 1$ if $(y_1, \ldots, yn) = \pi_S(x_1, \ldots, xm)$
- Compute the bias of a random variable using the formulas stated above....
- Example 4.2:
- consider the random variable $X1 \oplus X4 \oplus Y2$.
- The probability that this random variable takes on the value 0 can be determined by counting the number of rows in the table in which $X_1 \oplus X_4 \oplus Y_2$ = 0, and then dividing by 16.

Random variables defined by an S-box

- $\Pr[X_1 \oplus X_4 \ \oplus \ Y_2 = 0]$ =0.5
- The bias of this random variable is 0.

- $\Pr[X_3 \oplus X_4 \ \oplus Y_1 \ \oplus Y_4 = 0] = 0.125$
- The bias of this random variable is -0.375

X_1	X_2	X_3	X_4	Y_1	Y_2	Y_3	Y_4
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	1	0	1
0	0	1	1	0	0	0	1
0	1	0	0	0	0	1	0
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	0	0	0
1	0	0	0	0	0	1	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	0
1	0	1	1	1	1	0	0
1	1	0	0	0	1	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	0	0
1	1	1	1	0	1	1	1

Linear approximation table: values of $N_L(a,b)$

$$\left(\bigoplus_{i=1}^{4} a_i \mathbf{X_i}\right) \oplus \left(\bigoplus_{i=1}^{4} b_i \mathbf{Y_i}\right)$$

- The random variable $X_1 \oplus X_4 \oplus Y_2$. The input sum is (1, 0, 0, 1), which is 9 in hexadecimal;
- the output sum is (0, 1, 0, 0), which is 4 in hexadecimal.
- $\epsilon(a,b) = \frac{N_L(a,b) - 8}{16}$
- We computed $N_L(9,4) = 8$, and hence ϵ(9, 4) = 0

Linear approximation table: values of $N_L(a, b)$

	b															
a	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

Linear Cryptanalysis: informally describing

- Find a probabilistic linear relationship between a subset of plaintext bits and a subset of state bits immediately preceding the substitutions performed in the last round.
- There exists a subset of bits whose exclusive-or behaves in a non-random fashion (it takes on the value 0, say, with probability bounded away from 1/2).
- Assume that an attacker has a large number of plaintext-ciphertext pairs, all of which are encrypted using the same unknown key K (i.e., we consider a known-plaintext attack)

Linear Cryptanalysis

- For each of the plaintext-ciphertext pairs, we will begin to decrypt the ciphertext, using all possible candidate keys for the last round of the cipher.
- For each candidate key, we compute the values of the relevant state bits involved in the linear relationship, and determine if the abovementioned linear relationship holds.

Linear Cryptanalysis

- Whenever it does, we increment a counter corresponding to the particular candidate key.
- At the end of this process, we hope that the candidate key that has a frequency count furthest from 1/2 times the number of plaintext-ciphertext pairs contains the correct values for these key bits.

Public-key cryptography

- Asymmetric cryptography, is the field of cryptographic systems that use pairs of related keys. Each key pair consists of a public key and a corresponding private key
- Security of public-key cryptography depends on keeping the private key secret; the public key can be openly distributed without compromising security
- In a public-key encryption system, anyone with a public key can encrypt a message, yielding a ciphertext, but only those who know the corresponding private key can decrypt the ciphertext to obtain the original message

Public-key cryptography