Cryptography Overview (Part 1)

jedimaestro@asu.edu

Why do we need crypto?

- Confidentiality of messages
  - (Crypto doesn’t hide the message’s existence, that’s steganography)
- Integrity of messages
  - If a bit gets changed in transit, we’d like to know
- Authenticity

Other properties we might like...

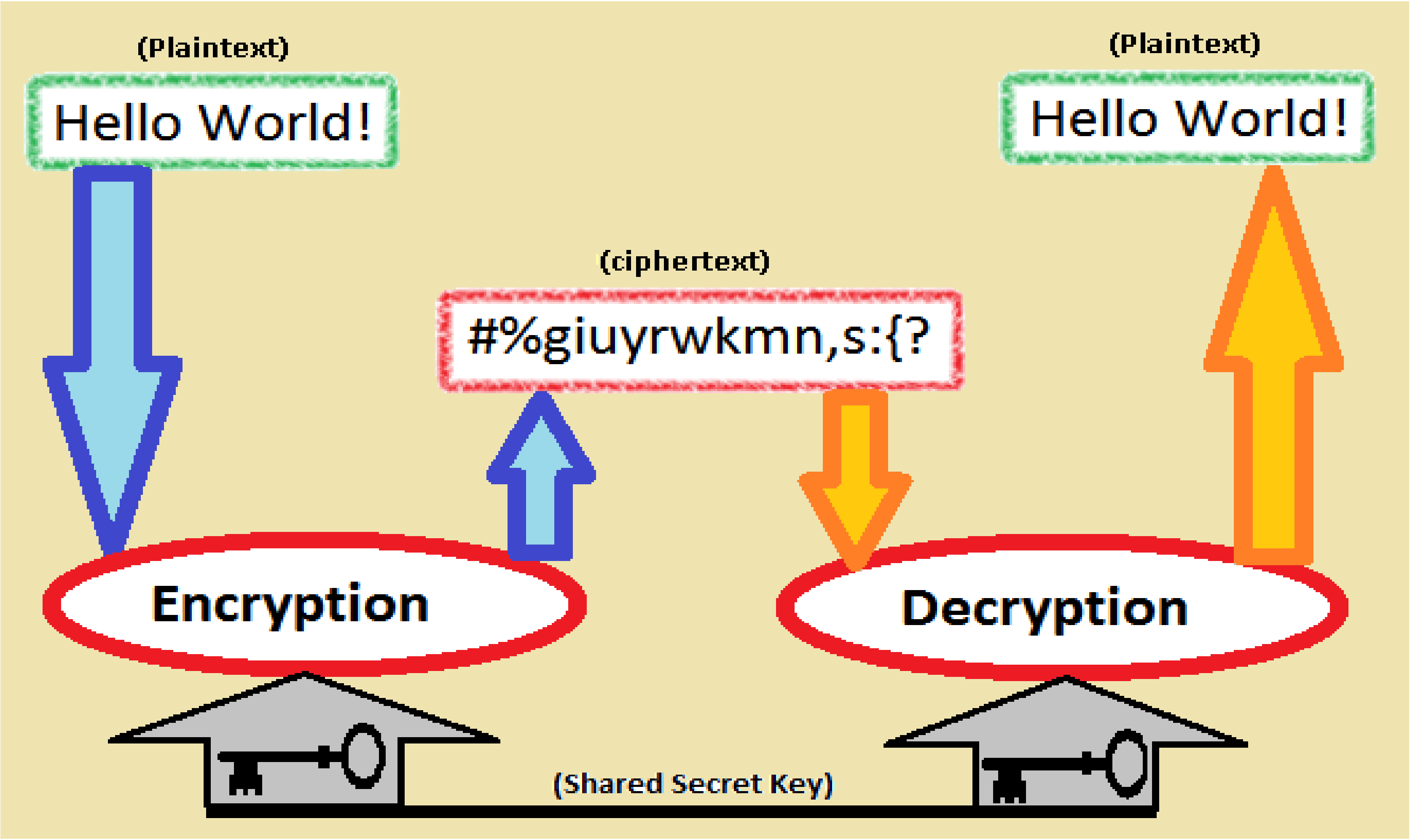
- Non-repudiation
- Off-the-record
  - Malleability, plausible deniability
- Future secrecy

Overview of this overview

- Symmetric encryption
  - Assumes two parties wishing to communicate already have a shared secret
- Asymmetric encryption
  - Makes different assumptions (*e.g.*, that everybody knows the public key or that the eavesdropper is passive)
- Secure hash functions and message authentication

Symmetric Crypto

- Confidentiality
- Integrity
- Authentication
- ~~Non-repudiation~~
- ~~A way to distribute the shared secret keys~~



Source: Wikipedia

Terminology

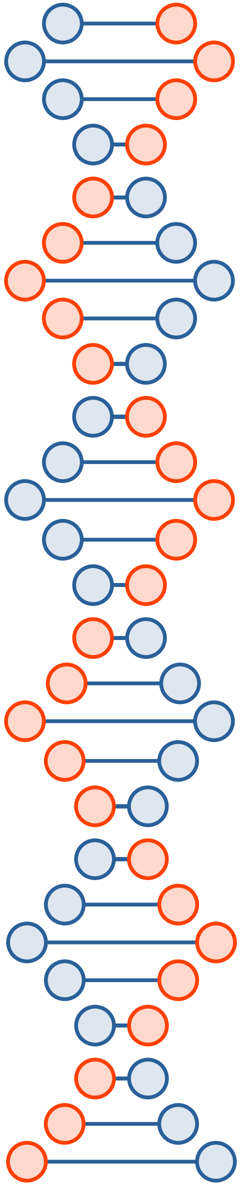
- Plaintext – before encryption, easy to read
- Ciphertext – after encryption, hopefully indecipherable without the key
- Key – the shared secret, typically just bits that were generated with a high entropy process

Review on your own...

- Caesar Cipher
- Vigenere Cipher and related attacks

Modern symmetric crypto

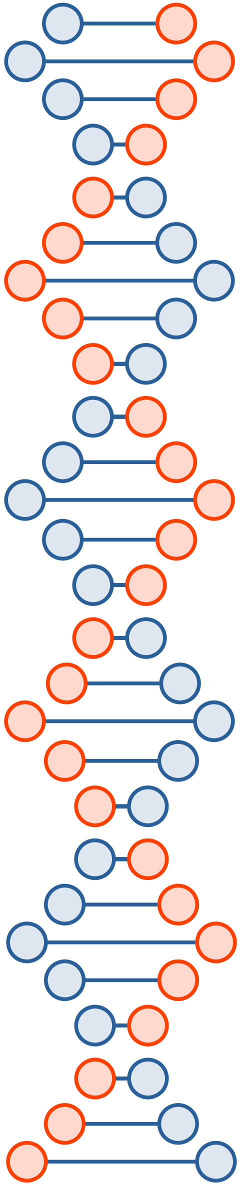
- Mostly:
  - Substitution
  - Permutation
  - XOR



Substitution

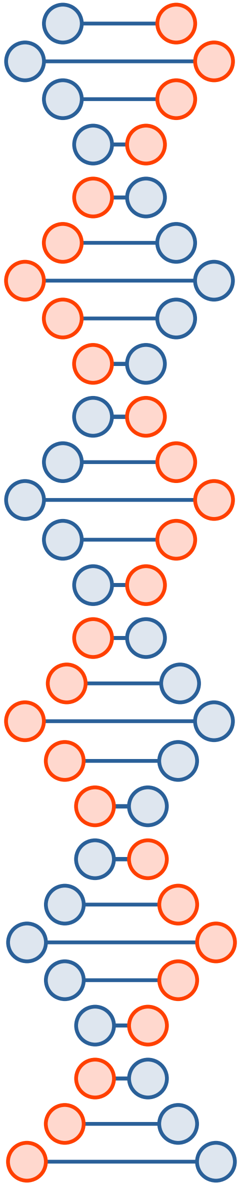
HELLO WORLD

TNWWX DXPWE



Permutation

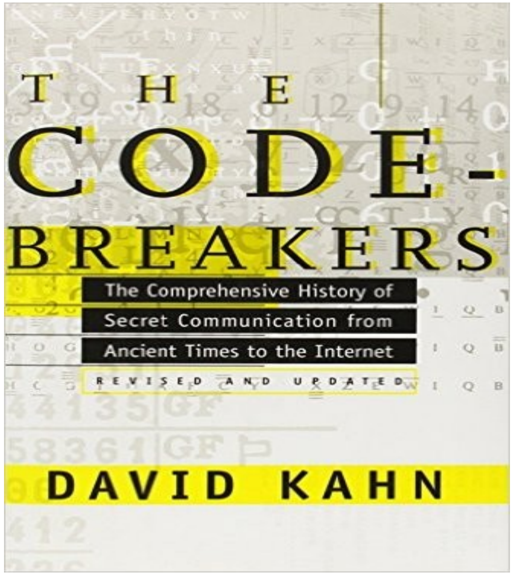
ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA



Bitwise XOR

$$
\begin{aligned}
&00101010_b \\
\oplus\, &10000110_b \\
=\, &10101100_b
\end{aligned}
$$

2000+ years of history...

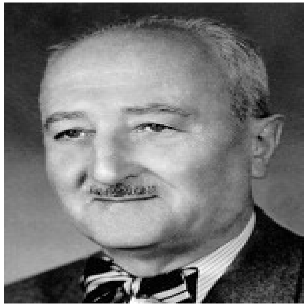


Symmetric encryption over time

- Handwritten notes, *etc.* for centuries
  - Typically the algorithm was secret
- 1883 … Kerckhoff’s rules
  - Now we know the key should be the only secret
- 1975 … DES
  - Efficient in hardware, not in software
- 2001 … AES
  - Efficient in software, and lots of different kinds of hardware

William and Elizabeth Friedman

- Met while analyzing Shakespeare ciphers at Riverbank Laboratories (“William Friedman wrote Shakespeare's plays”)
- Elizabeth solved ciphers of alcohol and drug smugglers, then German ambassadors in South America (three enigma machines)
- William led a team that solved PURPLE



Zodiac cipher

Image from wikia

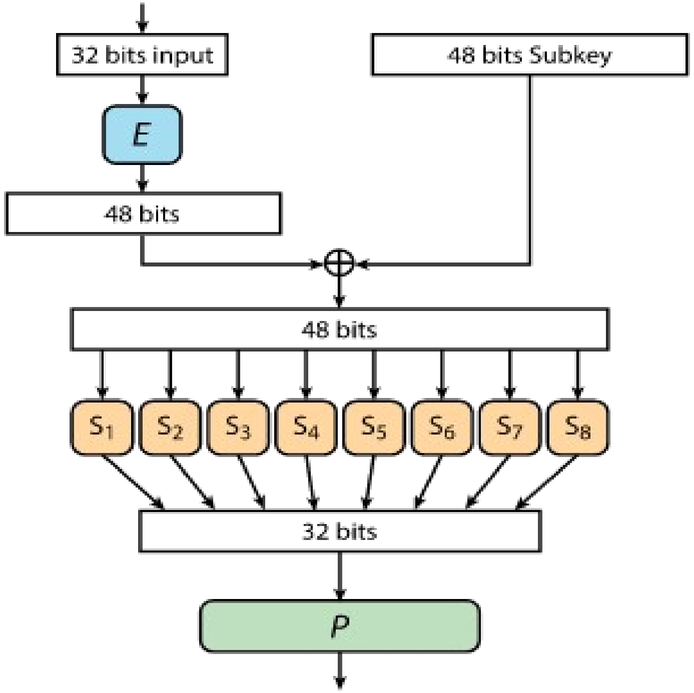
Modern symmetric crypto

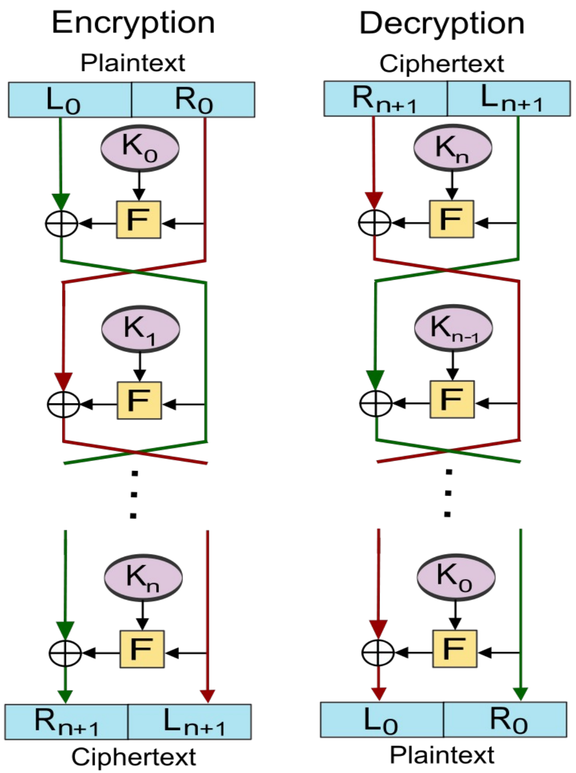
- Mostly:
  - Substitution
  - Permutation
  - XOR

Bitwise XOR as a cipher itself

- Typically used by malware, 8 or 32 bits
  - WEP attack uses these properties
- (B xor K) xor K = B
- (A xor K) xor (B xor K) = A xor B
- (0 xor K) = K
- (K xor K) = 0
- Frequency analysis or brute force

DES (16 rounds, 64-bit blocks, 56-bit key)





DES S-boxes

- 6 bits becomes 4 bits
- Somewhat arbitrary
  - IBM proposed some, NSA replaced with others

שורה	מס׳ עמודה															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
	S_5															
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
	S_6															
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
	S_7															
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
	S_8															
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Importance of substitution

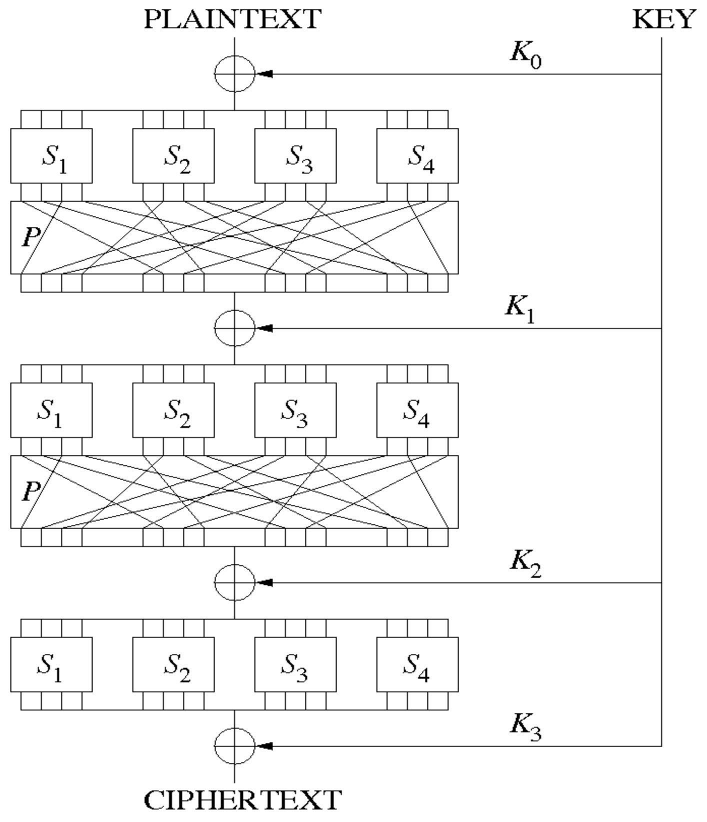
- XOR and permutation are linear functions
  - Solve for the key given plaintext and ciphertext?
- Bit differences in inputs are not changed at all by permuting bits
- XOR also preserves differences in bits

Different approaches

- DES simply tried to thwart these two specific types of attack (linear and differential) by carefully choosing the S boxes and letting them destroy information about the input (okay because of Feistel structure)
- AES is going to do something a lot more clever, that is invertible (no need for the Feistel structure, so fewer rounds) but still thwarts linear and differential cryptanalysis.
  - AES is covered in detail in CSE 539

Substitution Permutation Network

e.g., AES 128-bit blocks, (128-, 192-, 256-)bit key, (10, 12, 14) rounds



Block cipher *vs.* stream cipher

- Block cipher: break bits up into fixed-size chunks (pad if necessary)
  - Block cipher modes become important (ECB vs. CBC)
  - Detecting changes is relatively easy
- Stream cipher: Generate a pseudorandom key stream, combine it with the plaintext (typically using XOR)
  - Have to be careful not to reuse key material (known plaintext means key material can be recovered)
  - Have to be careful about authentication

Cipher modes

- ECB, CBC discussed on next slides
- Also Counter Mode, Galois Counter Mode, Cipher Feedback, Output Feedback
  - Parallelization and other features
  - Might be covered in CSE 539

Electronic Codebook (ECB)

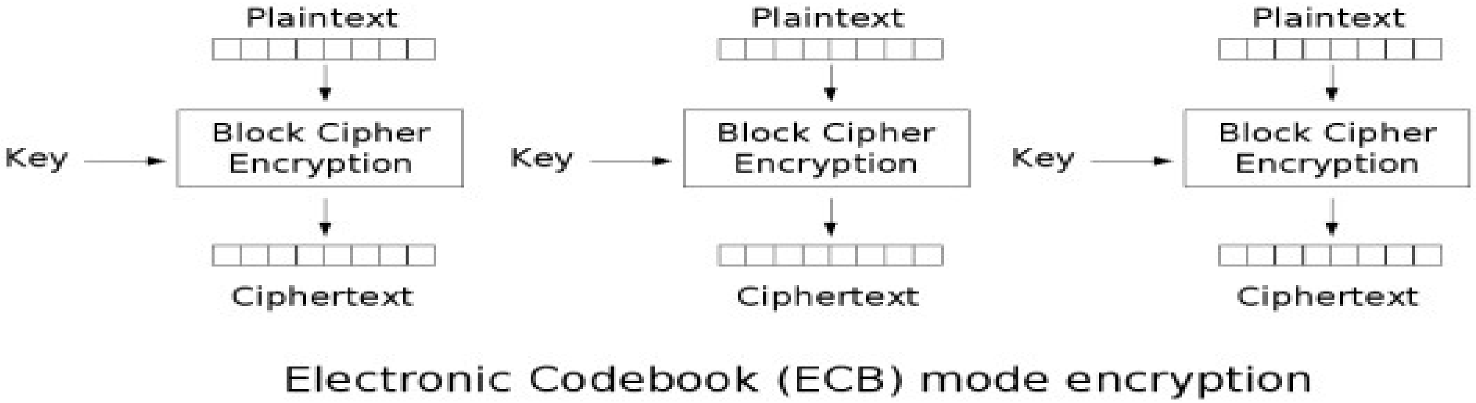
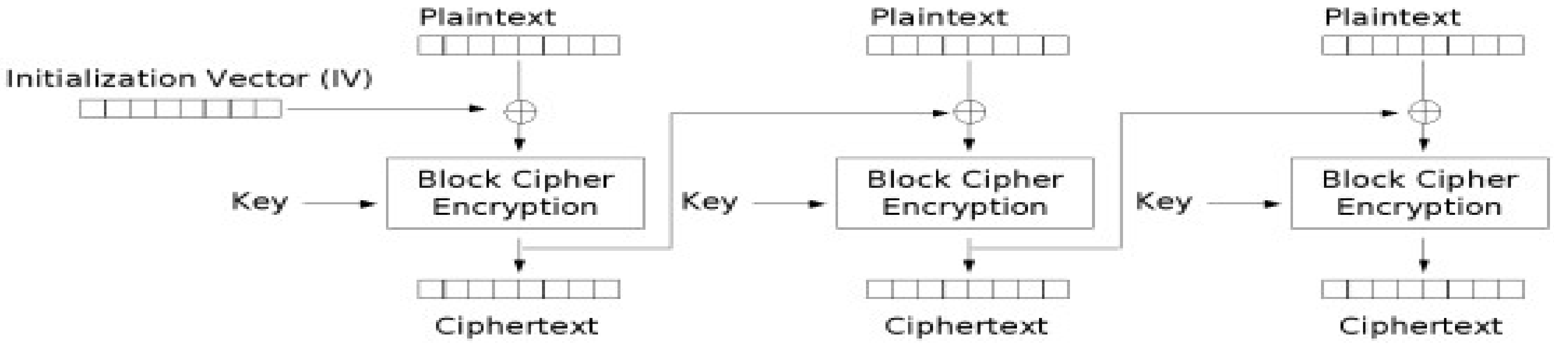


Image stolen from Wikipedia

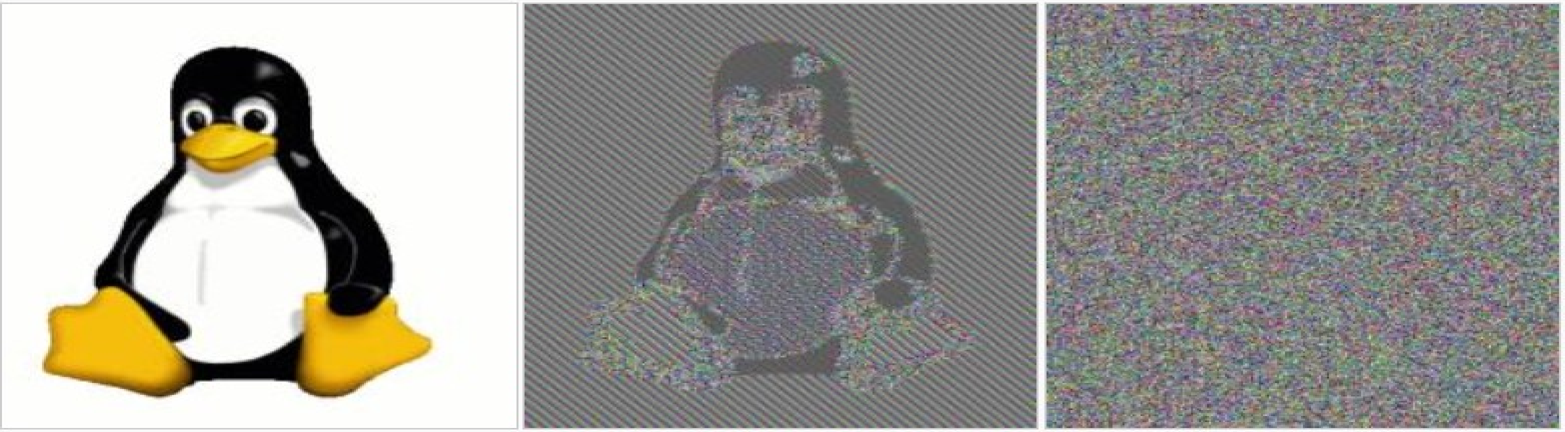
Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

Image stolen from Wikipedia

ECB is generally bad



Original image

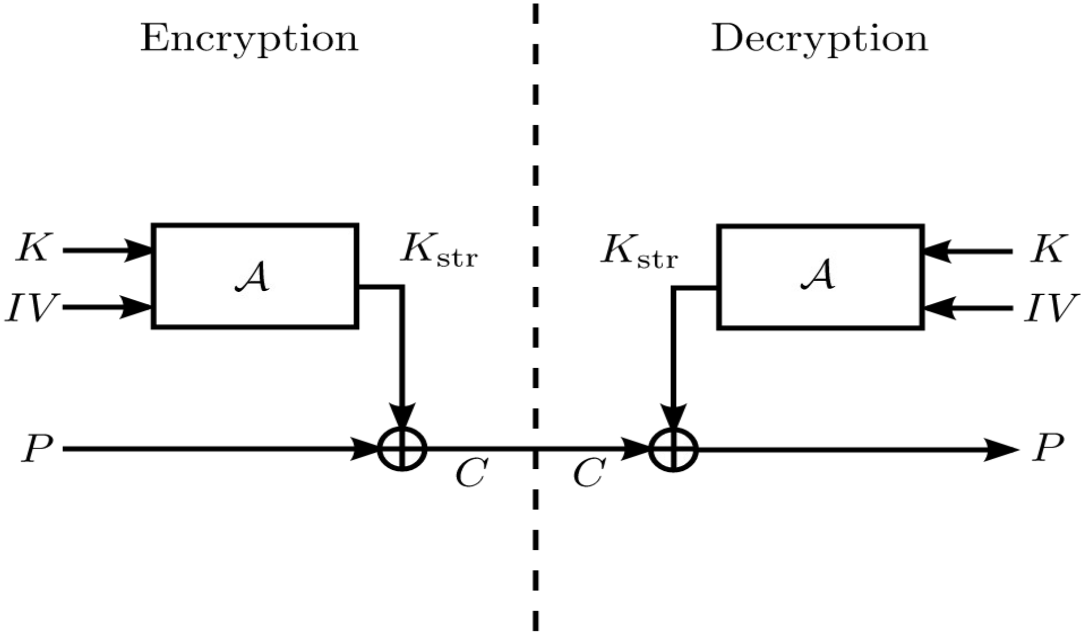
Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

The image on the right is how the image might appear encrypted with CBC, CTR or any of the other more secure modes—indistinguishable from random noise. Note that the random appearance of the image on the right does not ensure that the image has been securely encrypted; many kinds of insecure encryption have been developed which would produce output just as "random-looking".

Image stolen from Wikipedia

Stream cipher...



Coming up...

- An introduction to asymmetric encryption
- Secure hash functions and message authentication
- An attack on a stream cipher called RC4

Cryptography Engineering by Ferguson *et al.*