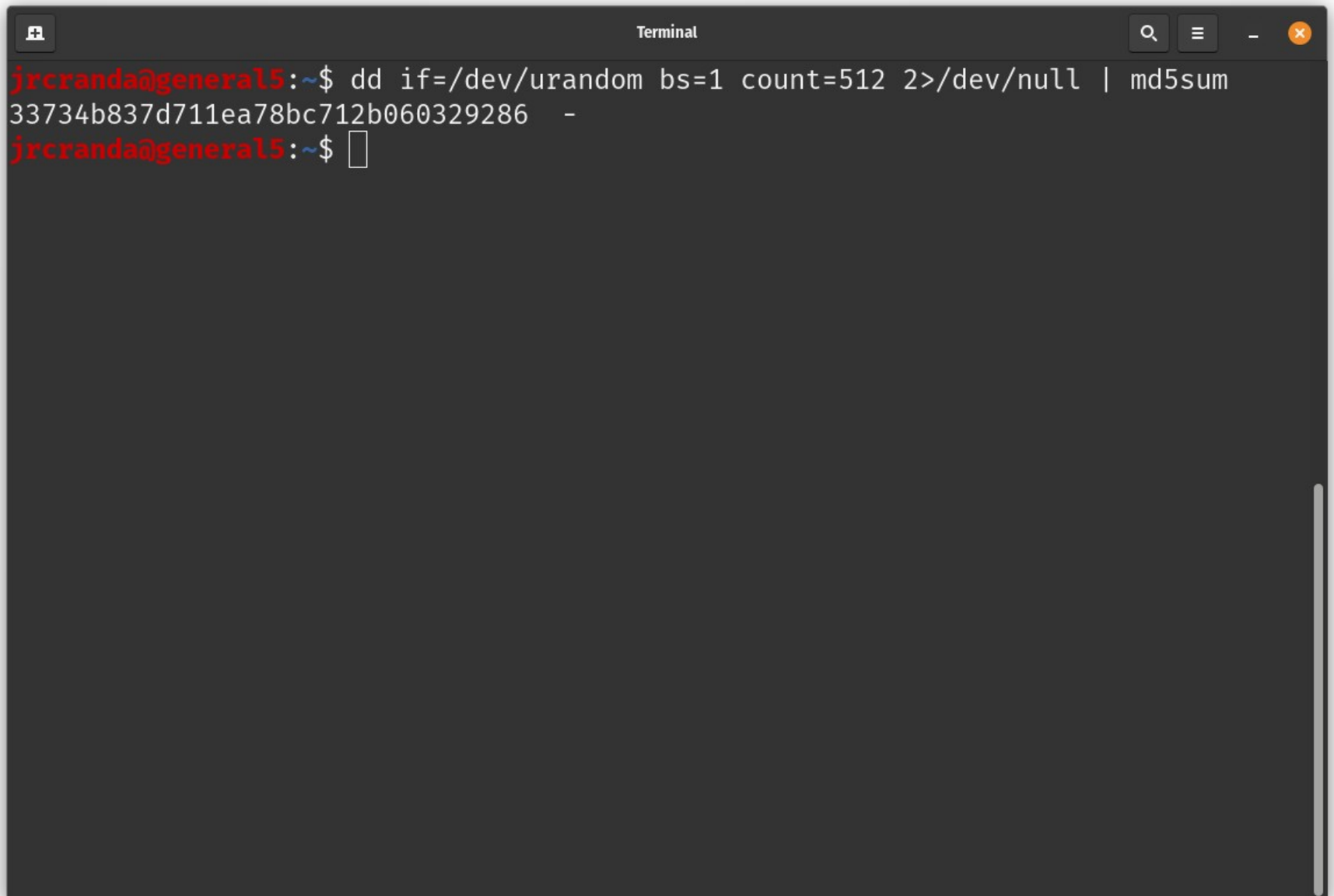
Crypto review…

Jed Crandall, jedimaestro@asu.edu

Administrativia

- Course website and syllabus
- Update: Wireshark + general.asu.edu + a programming environment is good enough

Example


Terminal
jrcranda@general5:~$ dd if=/dev/urandom bs=1 count=512 2>/dev/null | md5sum
33734b837d711ea78bc712b060329286 -
jrcranda@general5:~$

This should be review if you took CSE 365. If you need more review:

https://www.youtube.com/watch?v=KqqOXndnvic
https://www.youtube.com/watch?v=SkJcmCaHqS0
https://www.youtube.com/watch?v=QgHnr8-h0xI
https://www.youtube.com/watch?v=-dsKYoqwjT0

Review 1/3: Cryptographic hash functions…

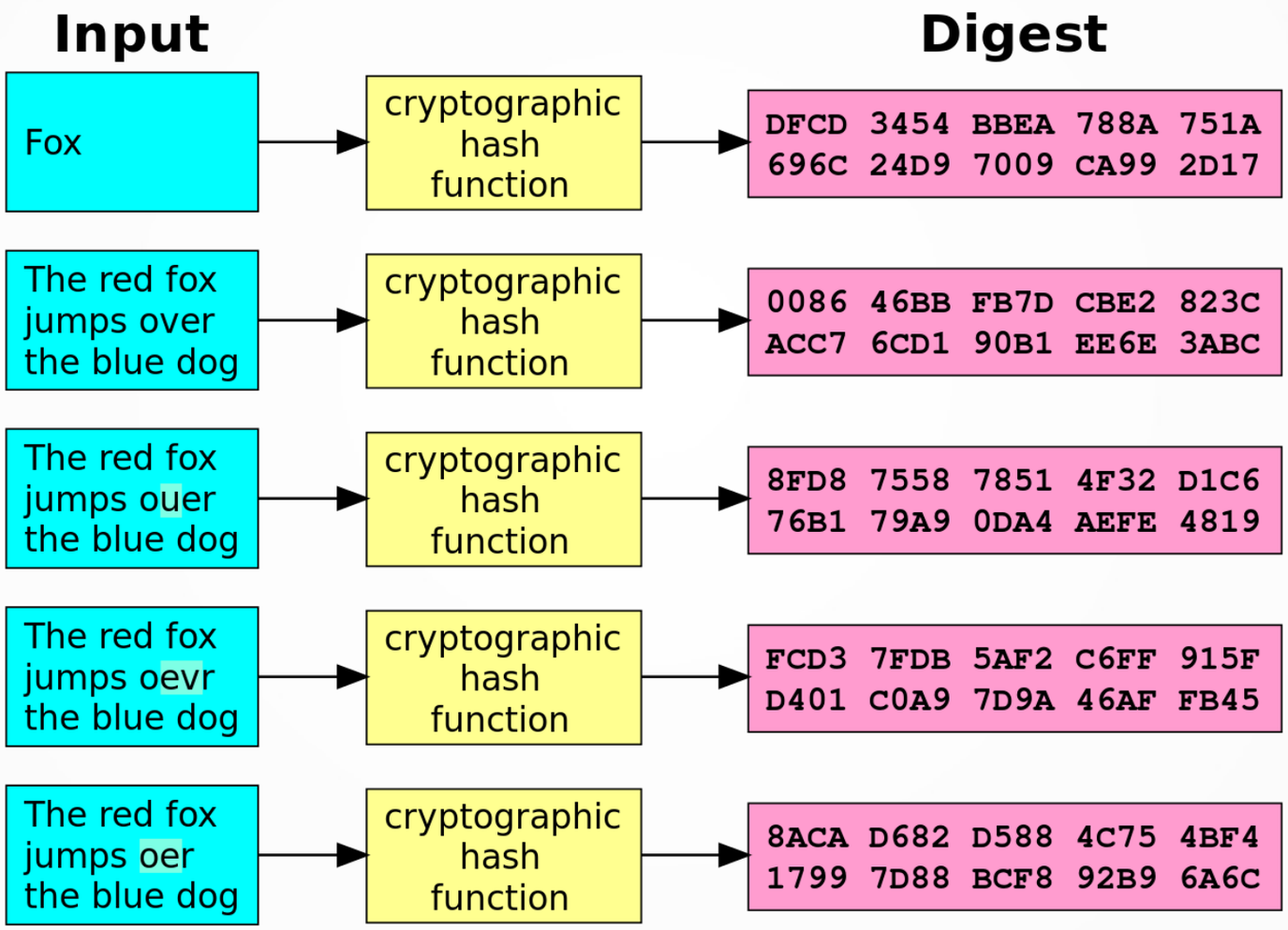
Why hash functions?

- Speed
- Error detection (*e.g.*, checksum)
- Security and privacy

Why cryptographic hash functions?

- Unique identifier for an object
- Integrity of an object
- Digital signatures
- Passwords
- Proof of work

Example



By User:Jorge Stolfi based on Image:Hash_function.svg by Helix84 - Original work for Wikipedia, Public Domain, https://commons.wikimedia.org/w/index.php?curid=5290240

What makes a hash function cryptographic?

- One-way function
- Deterministic (same input, same output)
- Infeasible to find message that digests to specific hash value
- Infeasible to find two messages that digest to the same hash
- Avalanche effect (small change in message leads to big changes in digest---digests seemingly uncorrelated)
- *Still want it to be quick*

Algorithms

- MD5: 128-bit digest, seriously broken
- SHA-1: 160-bit digest, not secure against well-funded adversaries
- SHA-3: 224 to 512 bit digest, adopted in August of 2015
- CRC32: not cryptographic, very poor choice

Property #1

- Pre-image resistance
- Given *h*, it should be infeasible to find *m* such that *h = hash(m)*

Property #2

- Second pre-image resistance
- Given a message m_1, it should be infeasible to find another message m_2 such that...
  $hash(m_1) = hash(m_2)$

Property #3

- Collision resistance
- It should be infeasible to find two messages, m_1 *and* m_2 such that...
  $hash(m_1) = hash(m_2)$

Attacks

- Pre-image attack
- Collision attack
- Chosen-prefix collision attack
- Birthday attack

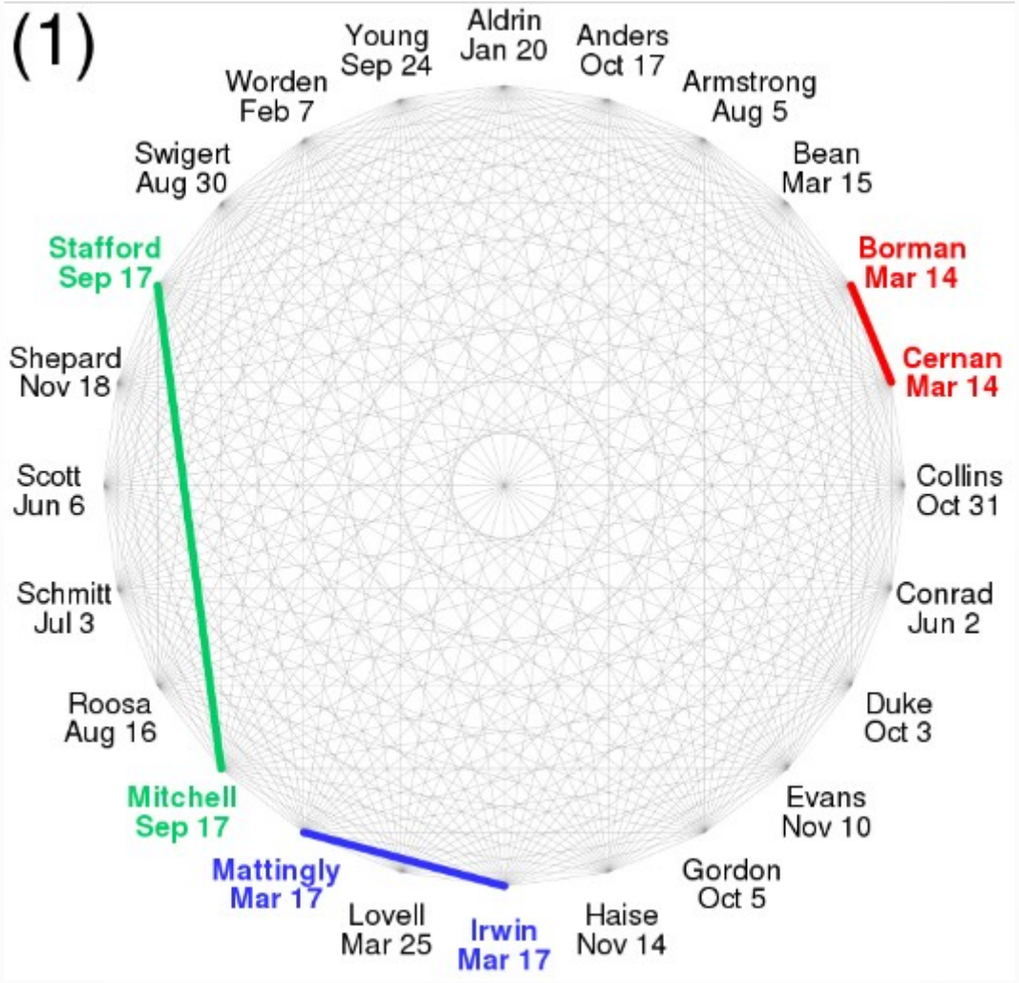
Chosen-prefix collision attack

- Given two prefixes p_1 and p_2, find m_1 and m_2 such that $hash(p_1||m_1)=hash(p_2||m_2)$
- p1 and p2 could be domain names in a certificate, images, PDFs, *etc. …* any digital image.
- This is one of the two ways MD5 is broken (other is plain old collision resistance), and is how we generated the two images with the same MD5 sum for the example from the Citizen Lab report

Birthday attack

- Probability of collision is *1* in 2^n, but the expected number of hashes until two of them collide is $sqrt(2^n)=2^{n/2}$
  - Why? Third try has two opportunities to collide, fourth has three opportunities, fifth has six, and so on...

24 people, same birthday?



https://commons.wikimedia.org/wiki/File:Birthday_attack_vs_paradox.svg

Think of a "random" 3-digit number

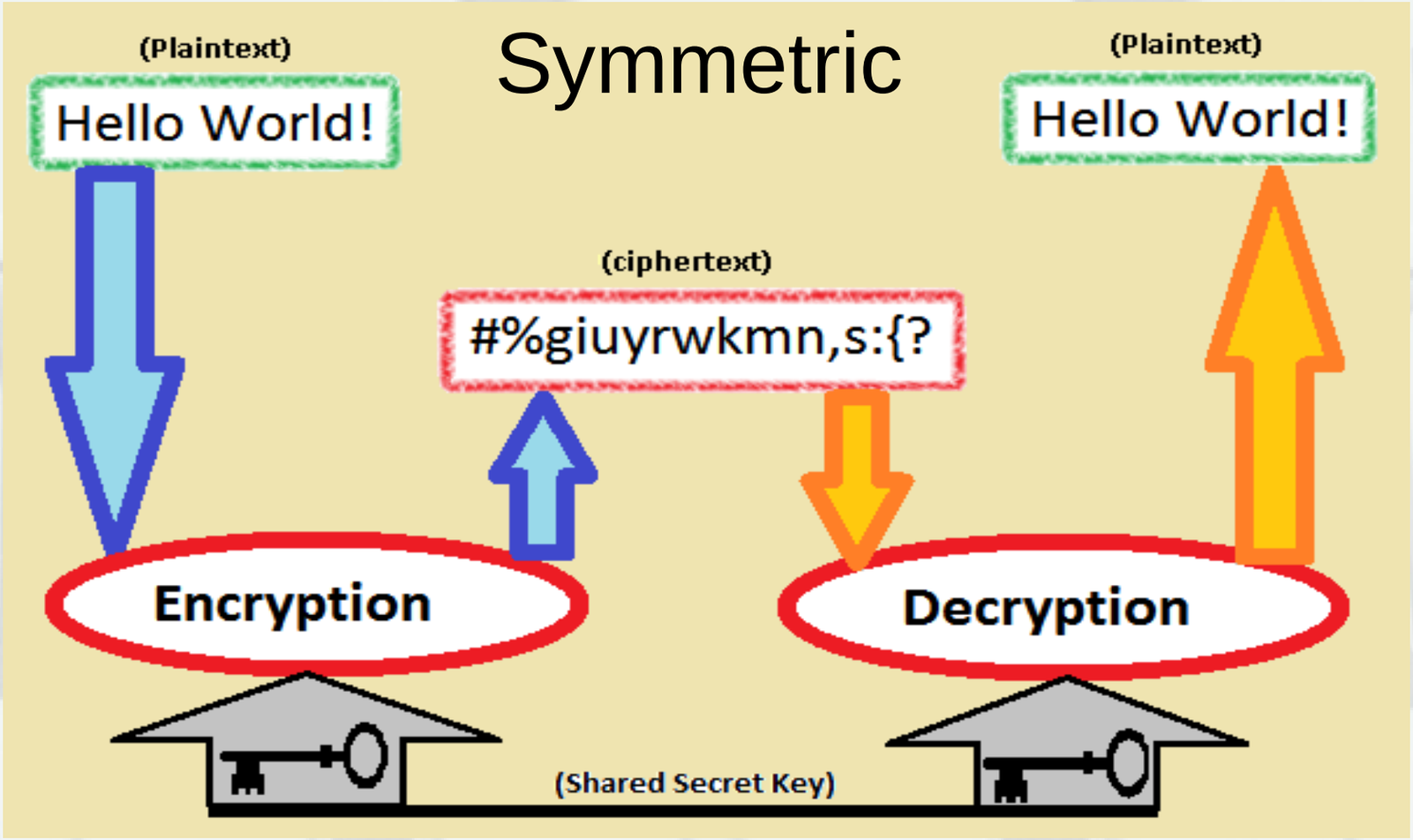
- *lg(999)* is a little under 10, so a 10-bit number
- $sqrt(2^{10})=2^5=32$
- You're going to say it out loud
  - We'll go around the room, go fast
  - Don't use your bank PIN, *etc.*
  - Raise your hand and yell if someone says your number

Review 2/3: Symmetric crypto

Symmetric crypto: same key on both sides

- Confidentiality
- Integrity
- Authentication
  - Compare to non-repudiation in asymmetric crypto

Symmetric



Source: Wikipedia

Review on your own…

- Caesar Cipher
- Viginere Cipher and related attacks

Modern crypto

- Mostly:
  - Substitution
  - Permutation
  - XOR

Substitution

HELLO WORLD

TNWWX DXPWE

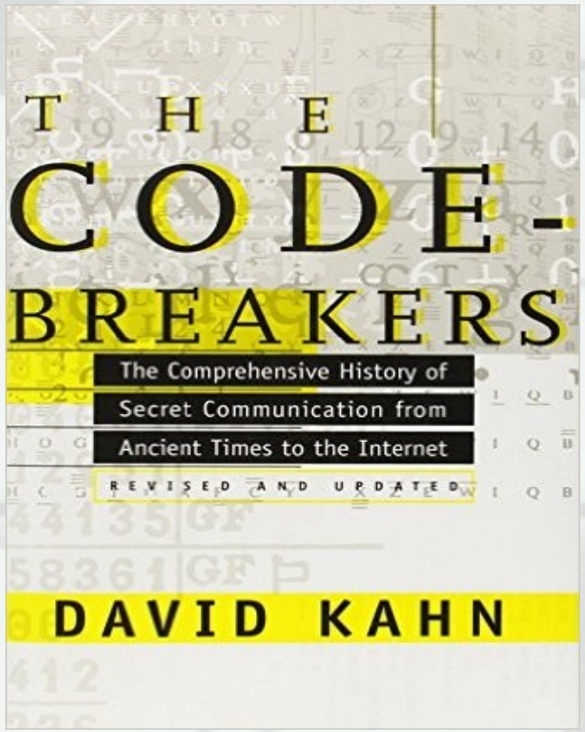
Permutation

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

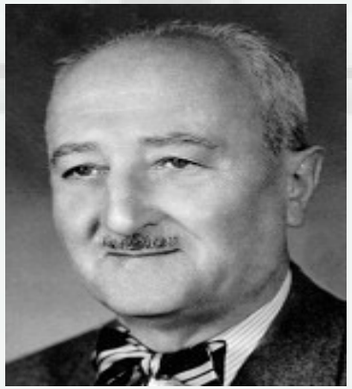
$$
\begin{aligned}
&00101010_b \\
\oplus\,&10000110_b \\
=\,&10101100_b
\end{aligned}
$$

2000+ years of history...



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



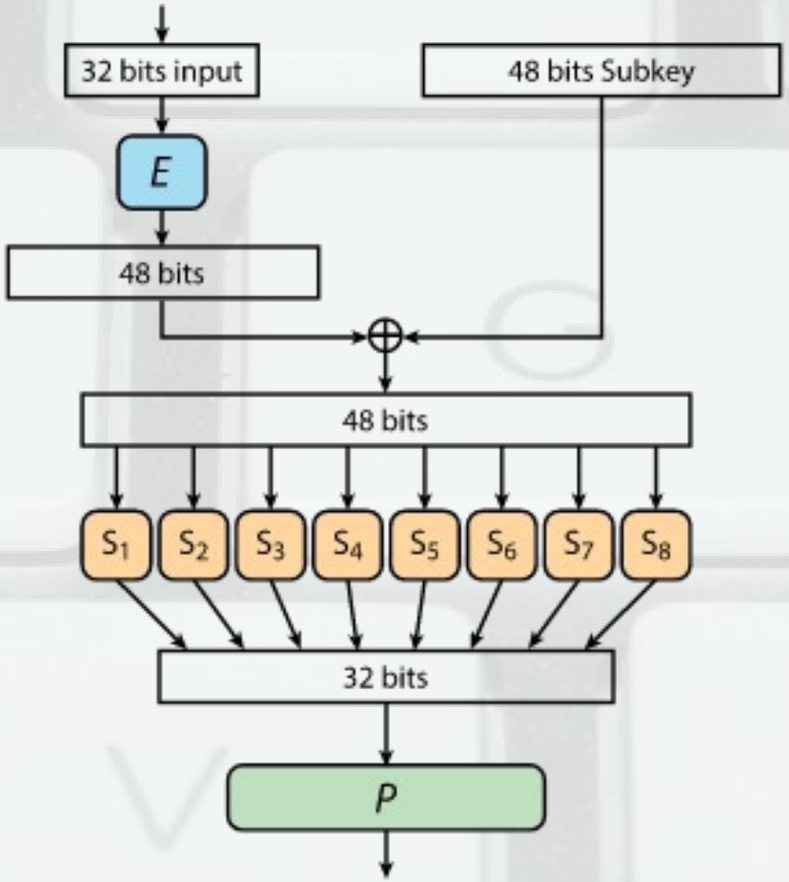
Zodiac cipher

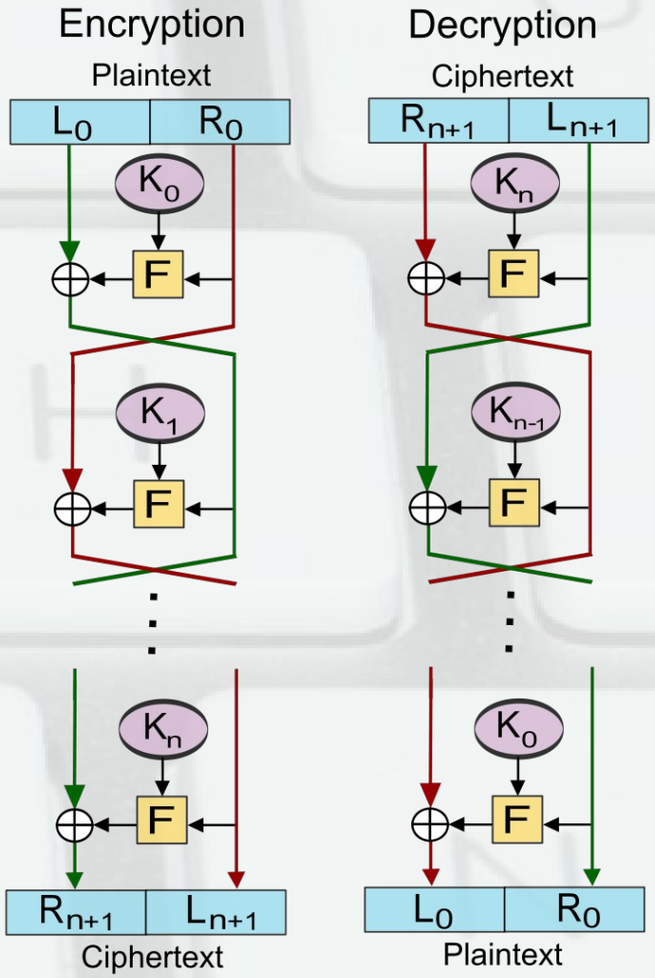
Image from wikia

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

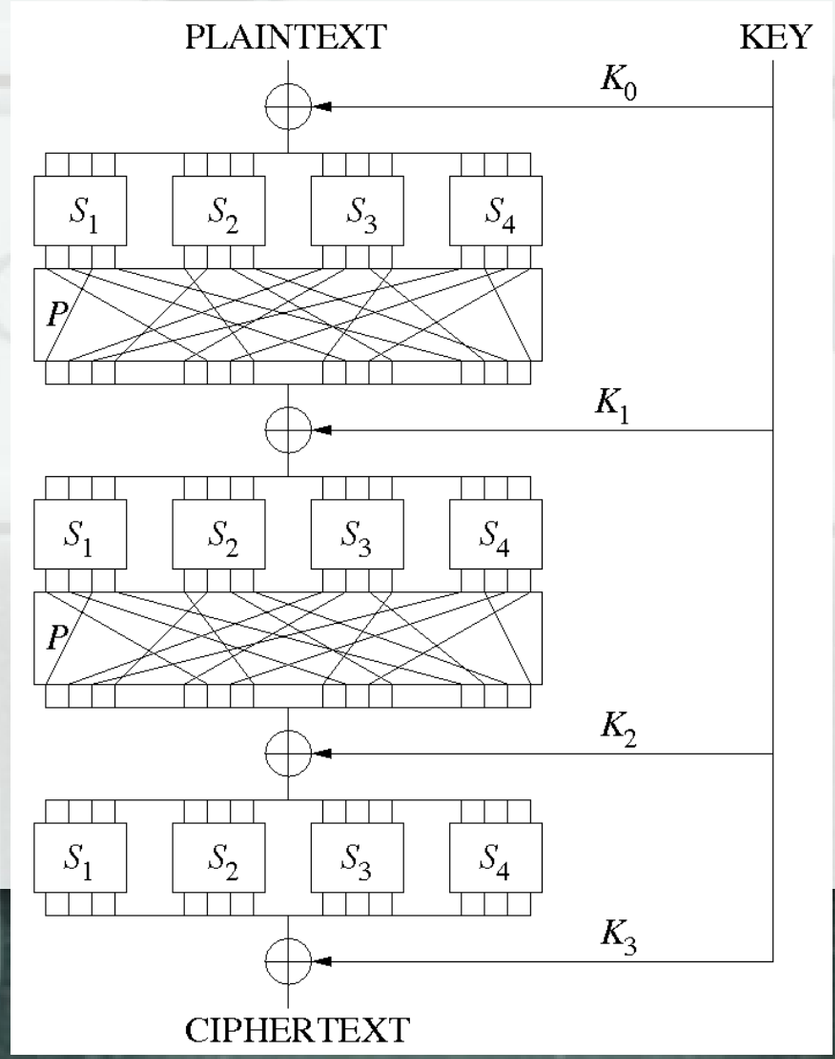
DES (16 rounds, 64-bit blocks, 56-bit key)



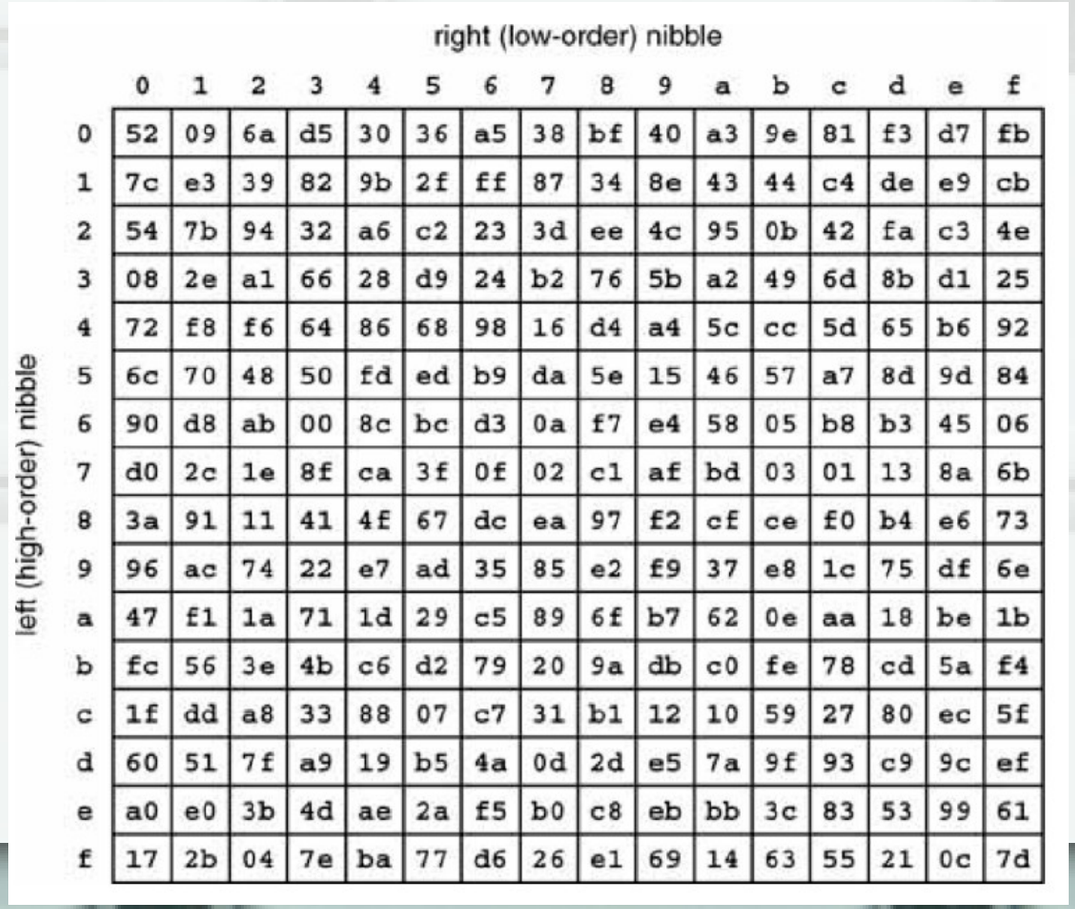


Substitution Permutation Network

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



An AES S-Box...



left (high-order) nibble	right (low-order) nibble															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

https://crypto.stackexchange.com/questions/55975/aes-s-box-input-and-output-question

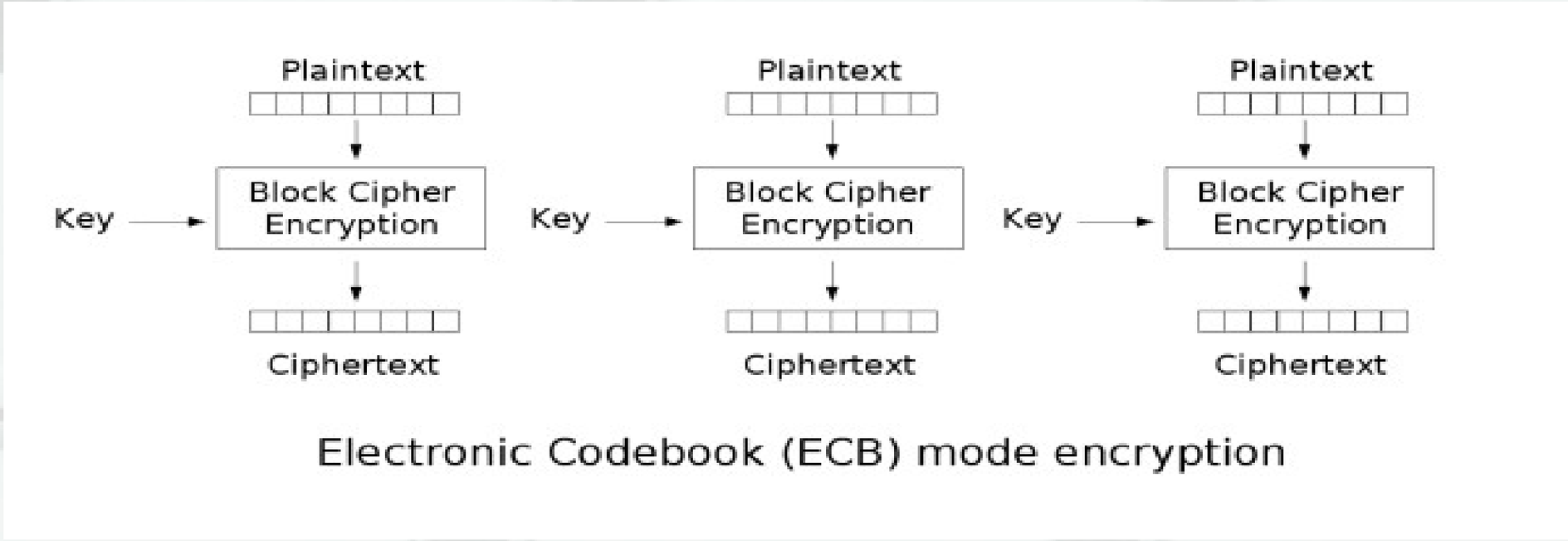
Block cipher *vs.* stream cipher

- Block cipher: break bits up into fixed-size chunks (pad if necessary)
- Stream cipher: Generate a pseudorandom key stream, combine it with the plaintext (typically using XOR)

Cipher modes

- ECB, CBC discussed on next slides
- Also Counter Mode, Galois Counter Mode, Cipher Feedback, Output Feedback
  - Parallelization and other features

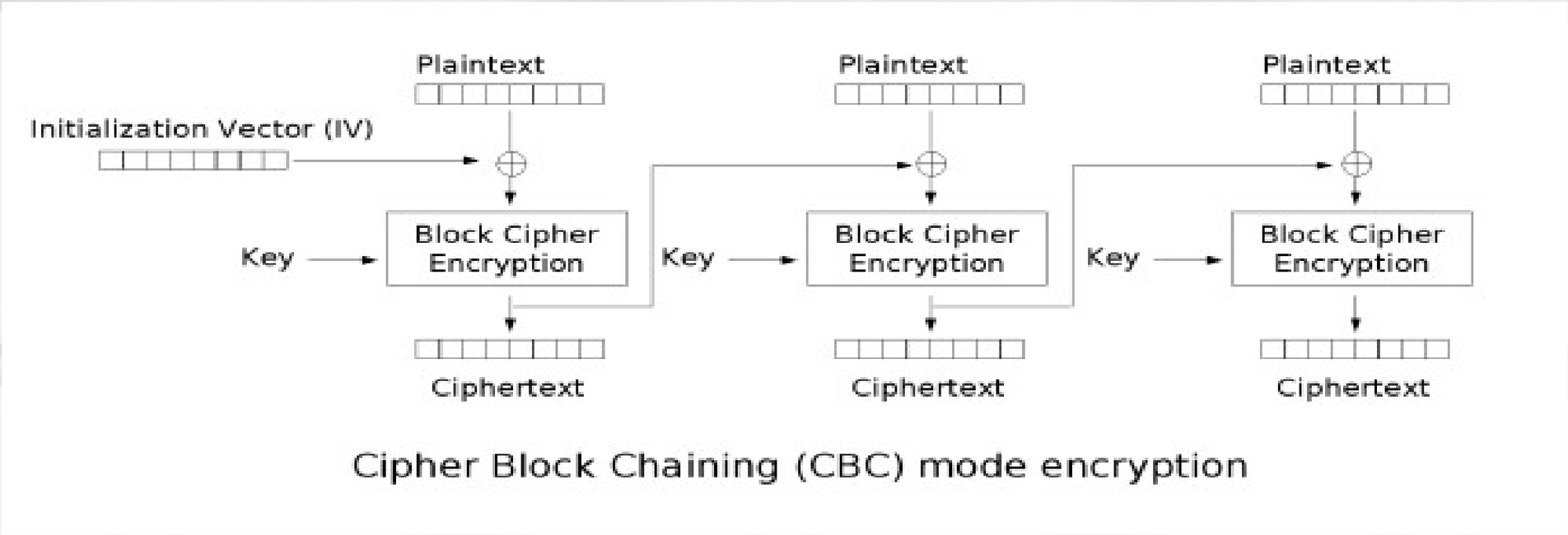
Electronic Codebook (ECB)



Electronic Codebook (ECB) mode encryption

Image stolen from Wikipedia

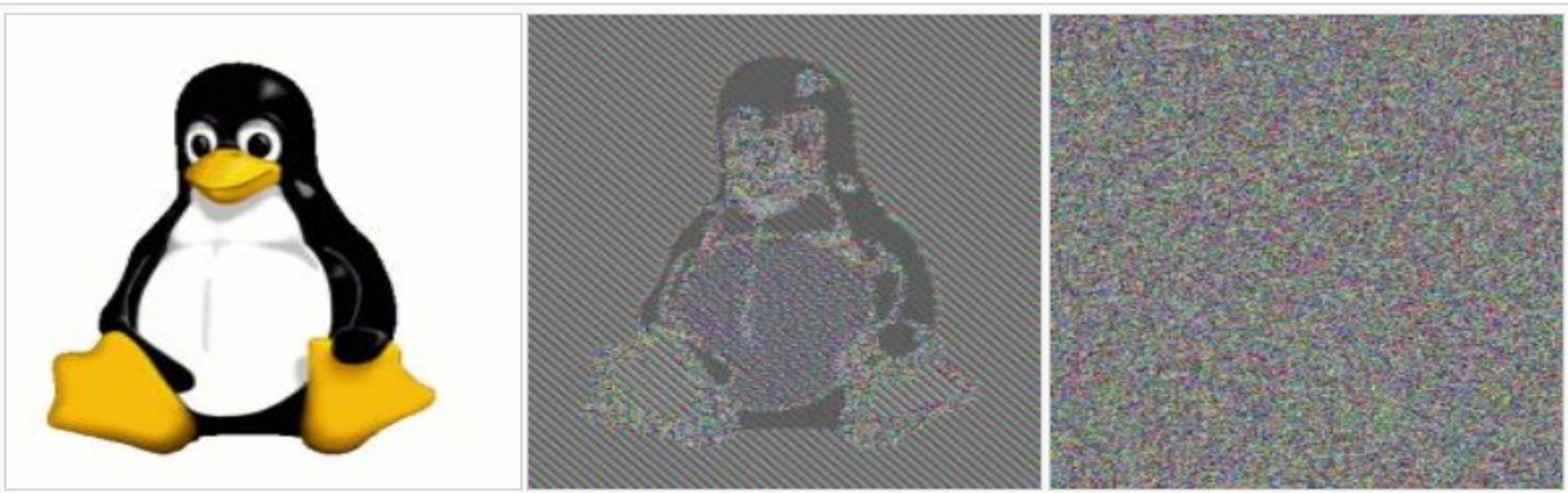
Cipher Block Chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

Image stolen from Wikipedia

ECB is generally bad

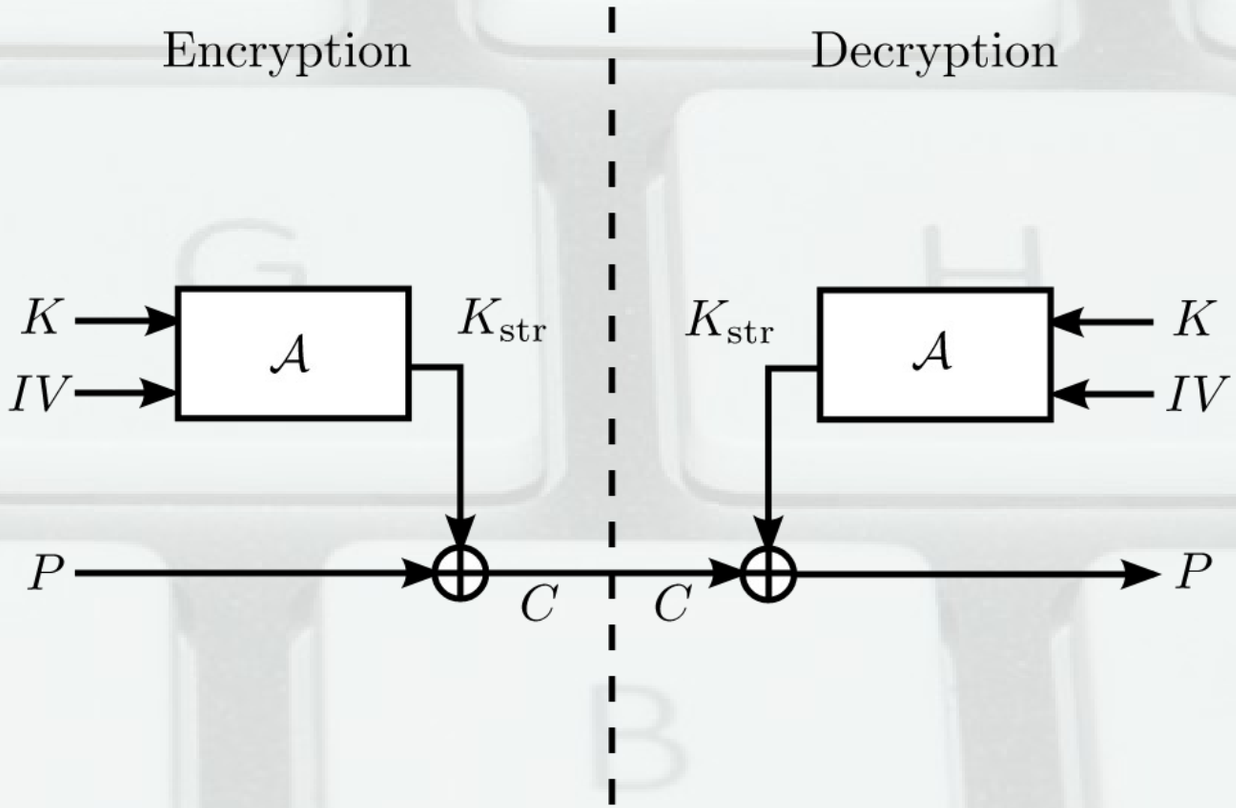


Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

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".

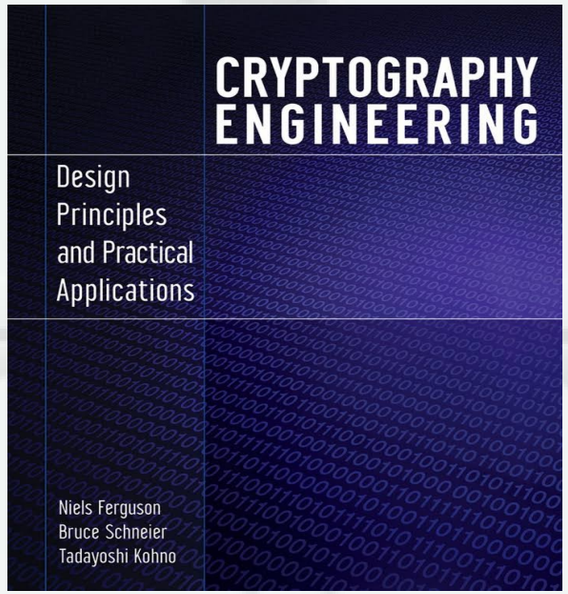
Image stolen from Wikipedia

Stream cipher...



Review 3/3: Asymmetric crypto… stay tuned

Cryptography Engineering by Ferguson *et al.*



Coming up...

- CBC padding oracle attack
  - Similar to RSA padding oracle attack from CSE 365
- RC4, WEP w/ attacks, WPA3
- Assymetric crypto, forward secrecy, Signal
- Transport Layer Security (TLS) and certificates
- Crypto FAILS

(Unless otherwise noted, all images are from Wikipedia)