CSE 484 / CSE M 584

Computer Security: Cryptography

TA: Franzi Roesner

franzi@cs.washington.edu

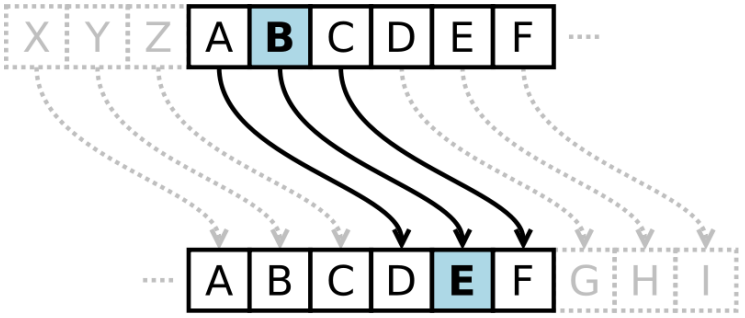
[Examples/Images thanks to Wikipedia.]

Lab 1 Deadline Reminders

- Lab 1 Final due next week (2/8, 5pm).
- Upcoming office hours:
  - Tomorrow (Friday) 10:30 am – Ian and Franzi
  - Monday 1:30 pm – Yoshi and Franzi
  - Wednesday 1:00 pm – Daseul and Ian
  - Thursday 12:30 pm – Franzi and Daseul

Caesar Cipher (Shift Cipher)

- Plaintext letters are replaced with letters a fixed shift away in the alphabet.



- Example:
  - Plaintext: `The quick brown fox jumps over the lazy dog.`
  - Key: Shift 3

    `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

    `DEFGHIJKLMNOPQRSTUVWXYZABC`

  - Ciphertext: `WKHTX LFNEU RZQIR AMXPS VRYHU WKHOD CBGRJ`

Caesar Cipher (Shift Cipher)

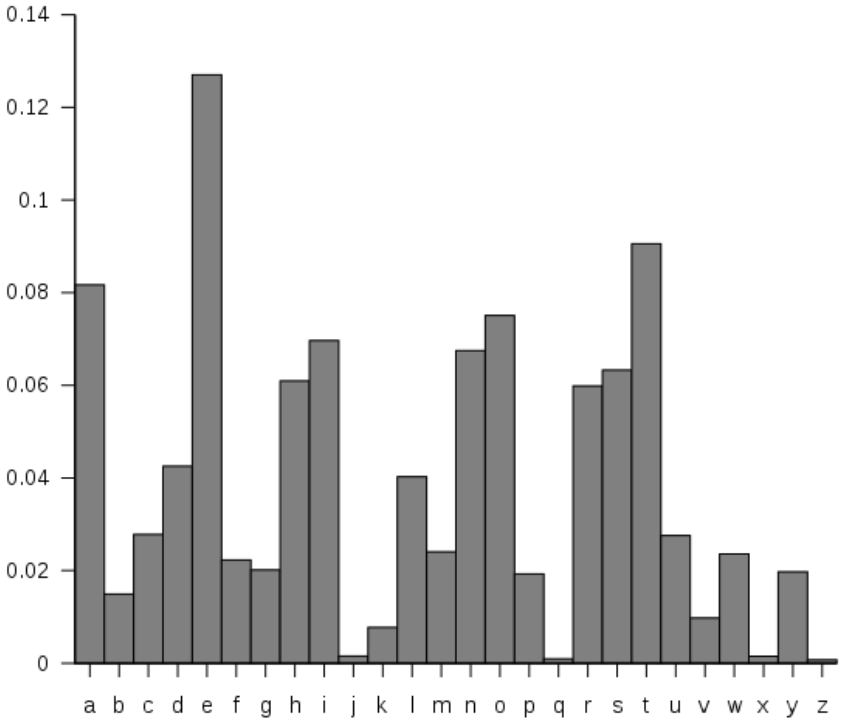
- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.

Substitution Cipher

- Superset of shift ciphers: each letter is substituted for another one.
- Monoalphabetic substitution cipher: fixed substitution over the entire message.
- Example:
  - Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Cipher: ZEBRASCDFGHIJKLMNOPQTUVWXY

Substitution Cipher

- What is the key space? 26! ~= 2^88
- How to attack?
  - Frequency analysis.



Bigrams:

th 1.52%	en 0.55%	ng 0.18%
he 1.28%	ed 0.53%	of 0.16%
in 0.94%	to 0.52%	al 0.09%
er 0.94%	it 0.50%	de 0.09%
an 0.82%	ou 0.50%	se 0.08%
re 0.68%	ea 0.47%	le 0.08%
nd 0.63%	hi 0.46%	sa 0.06%
at 0.59%	is 0.46%	si 0.05%
on 0.57%	or 0.43%	ar 0.04%
nt 0.56%	ti 0.34%	ve 0.04%
ha 0.56%	as 0.33%	ra 0.04%
es 0.56%	te 0.27%	ld 0.02%
st 0.55%	et 0.19%	ur 0.02%

Trigrams:

1. the	6. ion	11. nce
2. and	7. tio	12. edt
3. tha	8. for	13. tis
4. ent	9. nde	14. oft
5. ing	10. has	15. sth

Transposition Cipher

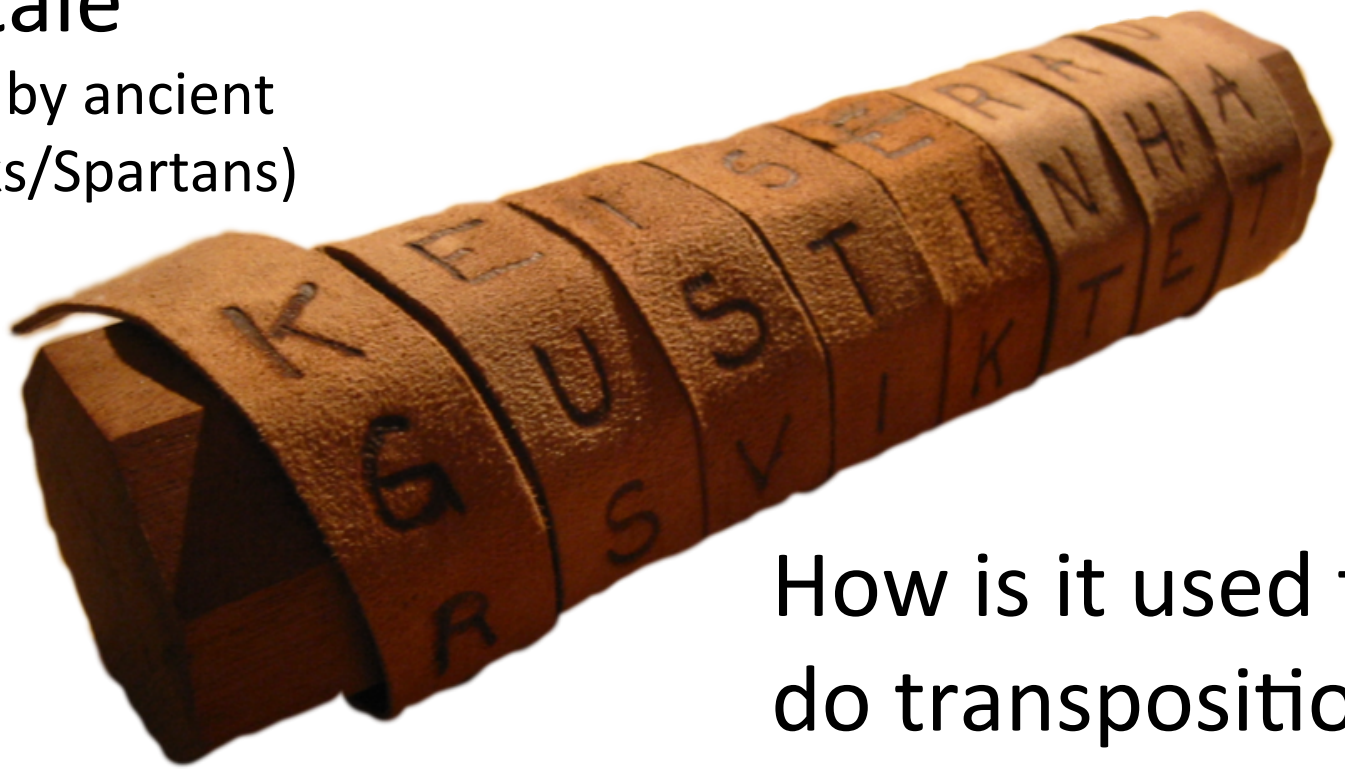
- Ciphertext is permutation of plaintext.
- Example: **Route cipher**
  - Plaintext: `WE ARE DISCOVERED, FLEE AT ONCE`
  - Arrangement:

    ```
    W R I O R F E O E
    E E S V E L A N J
    A D C E D E T C X
    ```

  - Key: "spiral inwards, clockwise, starting from top right"
  - Ciphertext: `EJXCTEDECDAEWRIORFEONALEVSE`

What is this?

Scytale
(used by ancient Greeks/Spartans)



How is it used to do transposition?

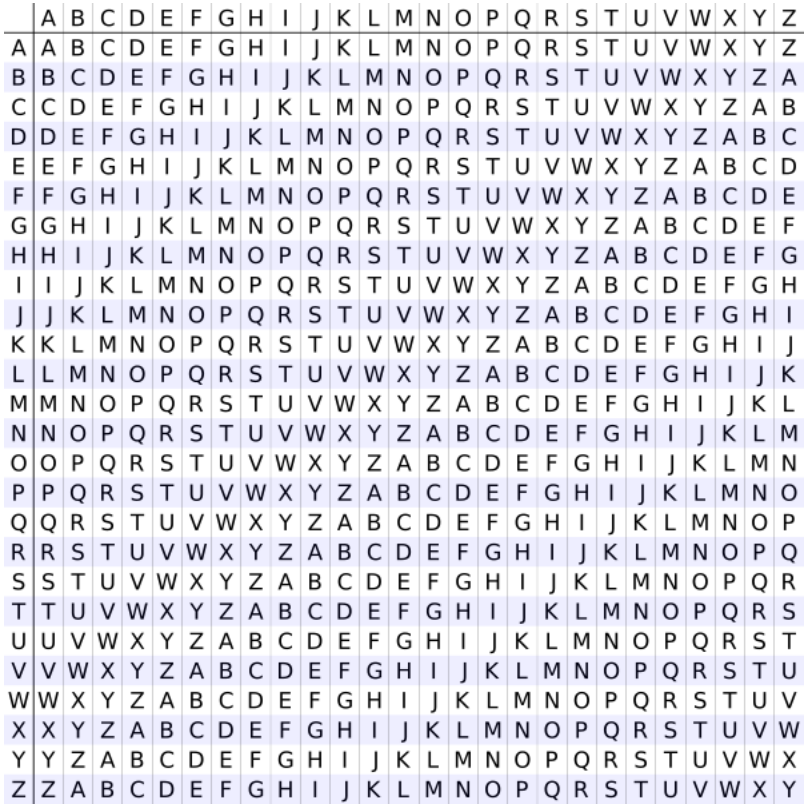
1. Wrap
2. Write horizontally
3. Encrypt = unwrap
4. Decrypt = rewrap

Transposition/Substitution

- How to tell if ciphertext was encrypted using substitution or transposition cipher?
  - If letter frequencies are normal, it's transposition.
- What happens if you combine substitution and transposition?
  - Substitution prevents anagram finding, transposition prevents digram/trigram analysis.

Vigenère Cipher (~1467)

- Polyalphabetic substitution cipher: use multiple substitution alphabets.
- Example:
  - Plaintext: `ATTACKATDAWN`
  - Key: `LEMONLEMONLE`
  - Ciphertext: `LXFOPVEFRNHR`
- Encrypt:
  - (Key-Row, Msg-Col)
  - Or just addition mod 26



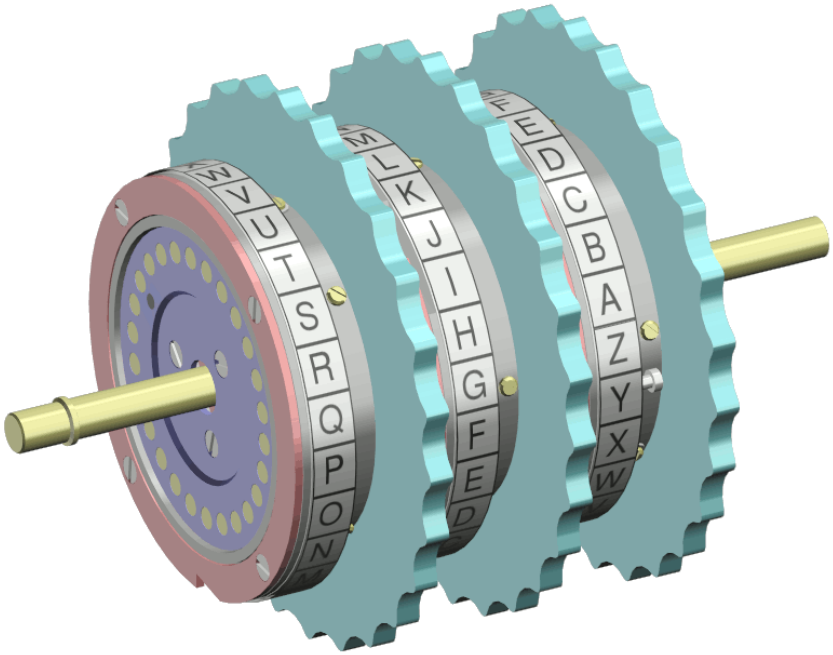
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Cipher (~1467)

- Does this defeat frequency analysis?
  - Not if you know the length of the (repeating) key (e.g., if key length = 5, do frequency analysis on set of every 5^{th} letter).
  - Even if you don't know the key length, just iterate with length=1…n until decryption looks sensible.
- What if the key doesn't repeat (i.e., length of key >= length of plaintext)?
  - One-time pad. (Same caveats: fully random key, use only once…)

Enigma Machine

Uses rotors (substitution cipher) that change position after each key.



Key = initial setting of rotors

Key space?

26^n for n rotors

Steganography

- Hidden messages (security through obscurity)

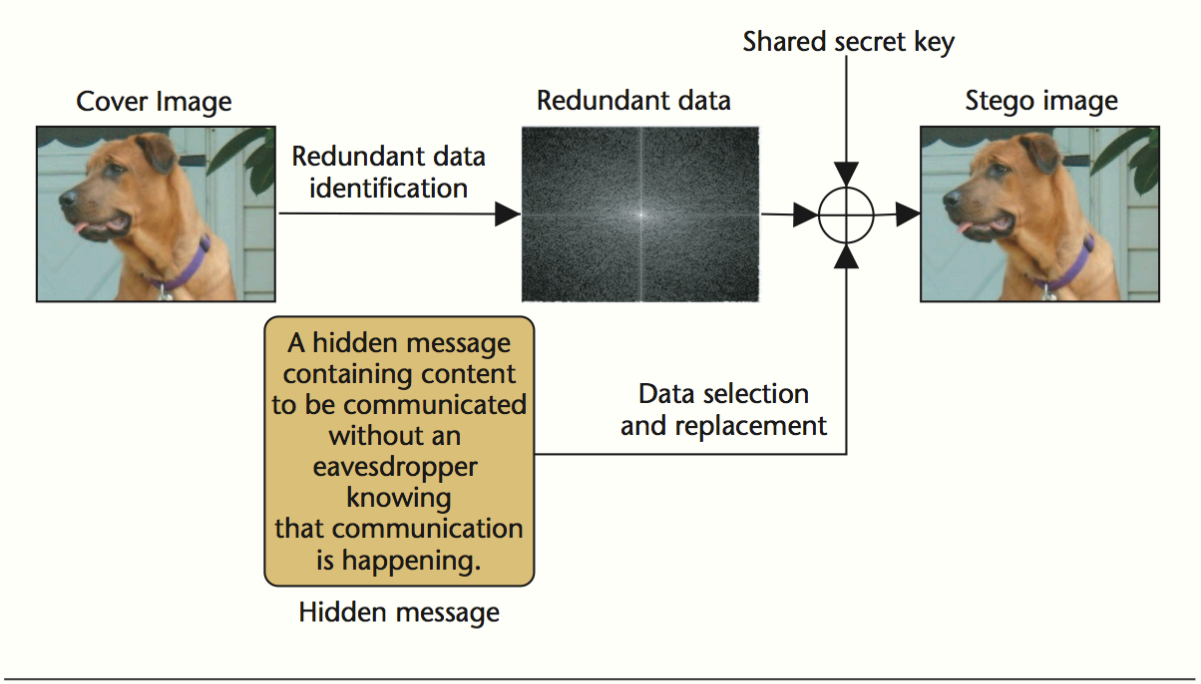
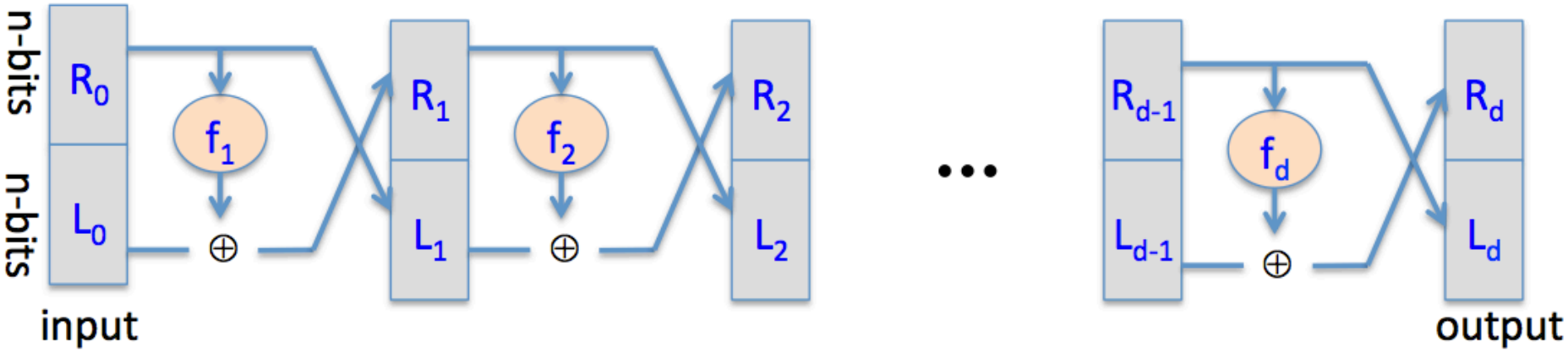


Figure 1. Modern steganographic communication. The encoding step of a steganographic system identifies redundant bits and then replaces a subset of them with data from a secret message.

[Figure from "Hide and Seek: An Introduction to Steganography" by Niels Provos and Peter Honeyman]

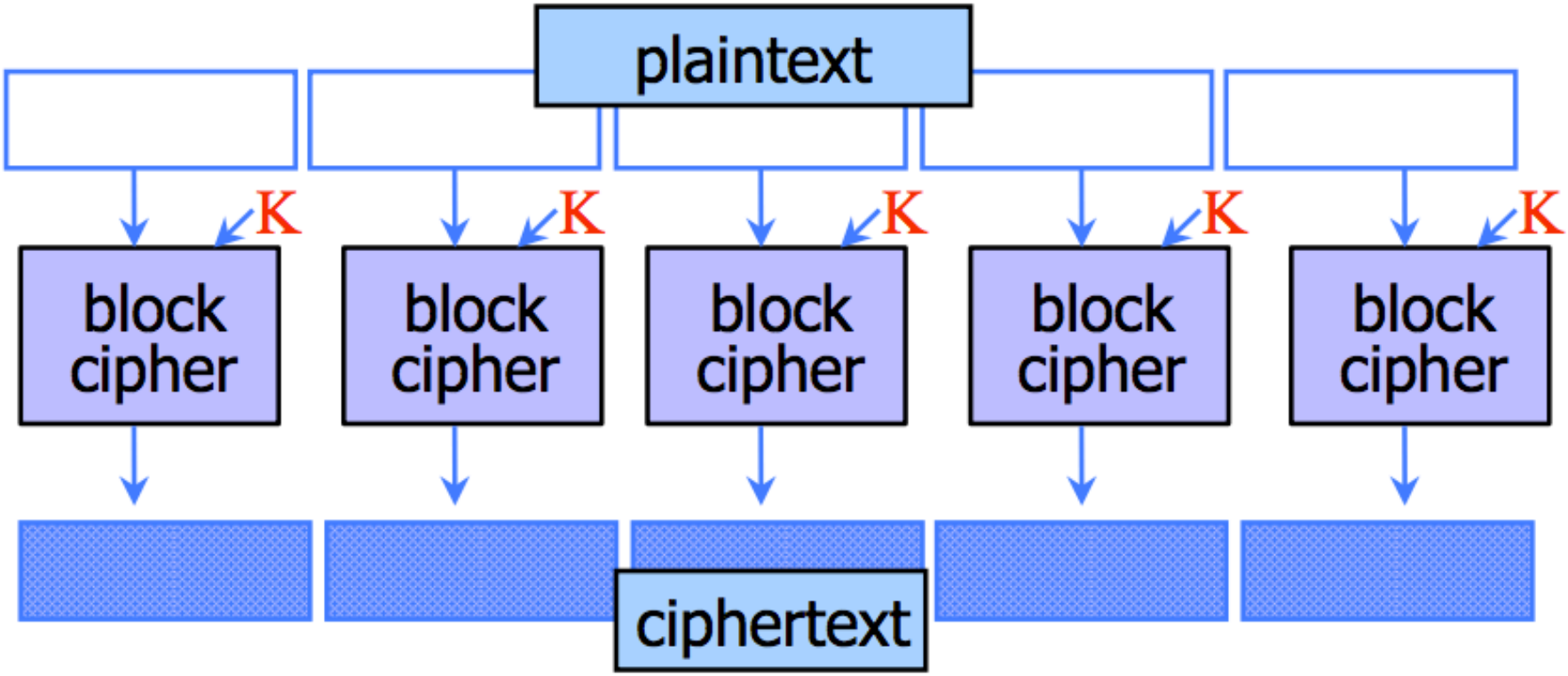
Feistel Network

- Important for DES (and others). What does it do?
  - Builds invertible function using non-invertible ones.



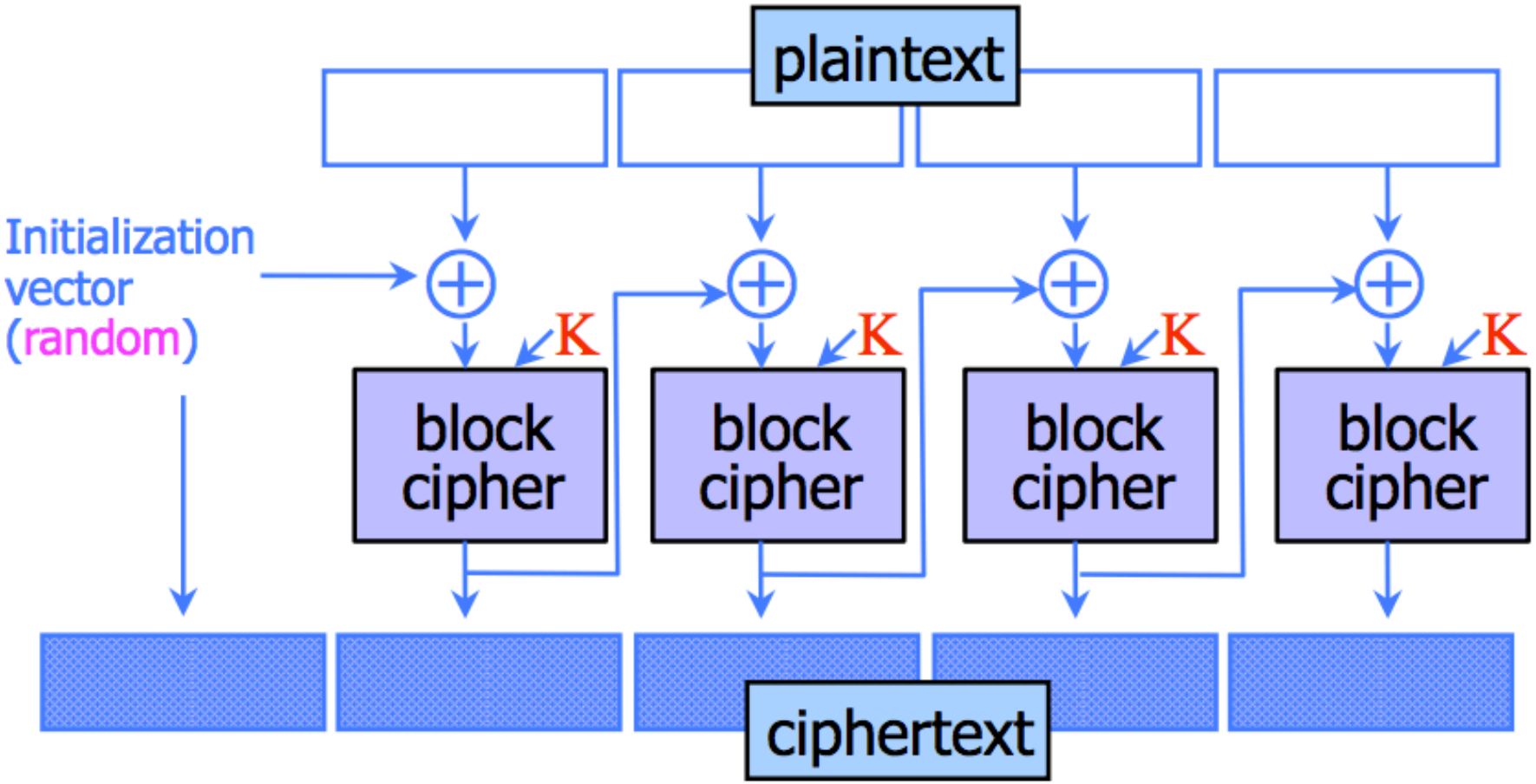
[Figure from Dan Boneh's slides]

Block Cipher Mode: ECB



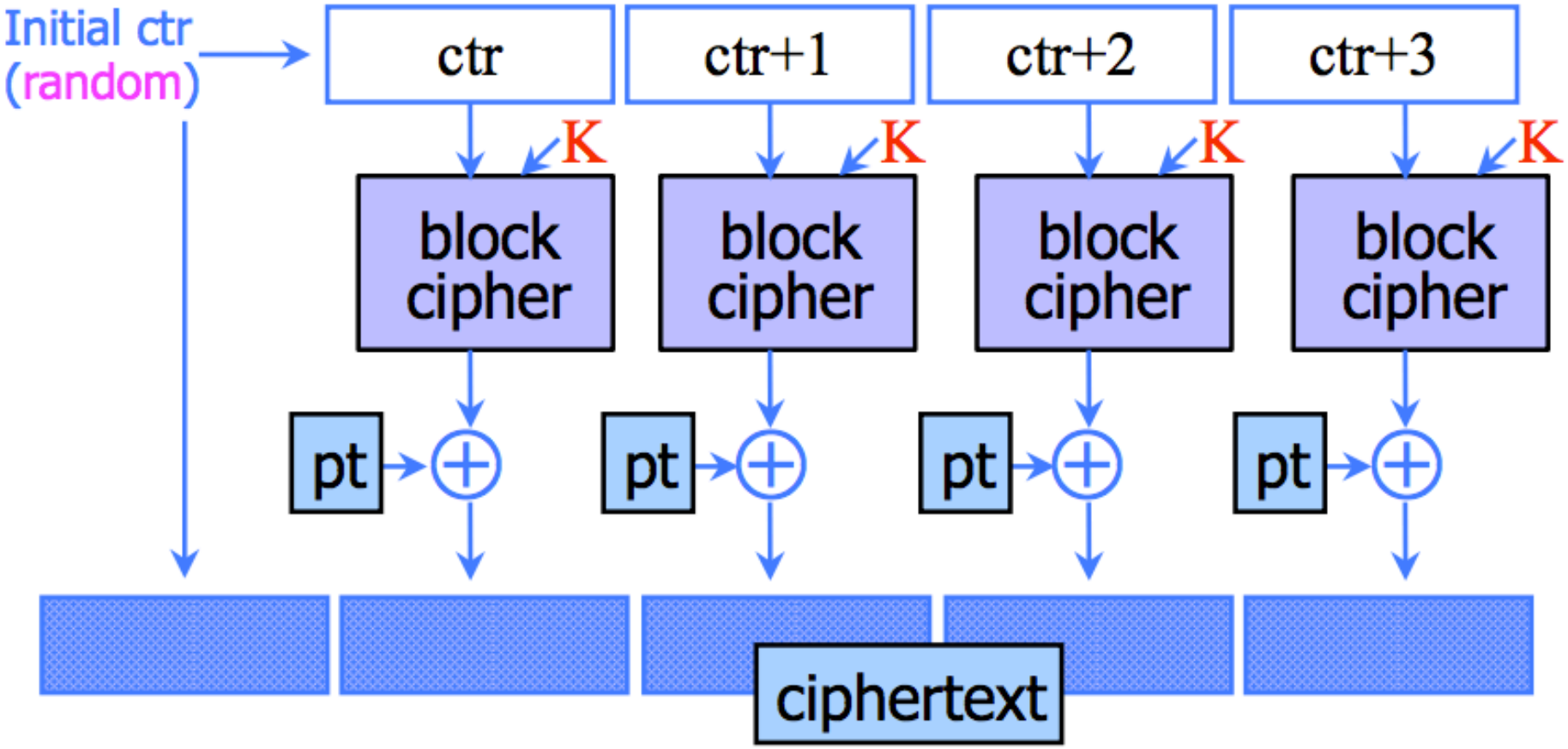
[Figure from Yoshi's slides]

Block Cipher Mode: CBC



[Figure from Yoshi's slides]

Block Cipher Mode: CTR



[Figure from Yoshi's slides]

Password Salting

- Servers shouldn't store passwords, but password hashes. (Why?)
- Threat: rainbow tables (pre-computed password hashes)
- Solution: salt
  - Each password is hashed/stored with a random value. Now a pre-computed table is useless.
  - Other benefits?

Additional Resources

- Stanford online crypto class: https://class.coursera.org/crypto-preview/class
- Books:
  - "The Codebreakers" by David Kahn
  - "The Code Book" by Simon Singh