CSE 484 / CSE M 584
Computer Security

TA: Jared Moore

jlcmoore@cs

Logistics

- Lab #1 due next Friday
- Today:
  - Lab 1 questions.
  - Authentication grab bag.
  - (if time) Cryptography

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?

Measuring Password Strength

- How many possible passwords are there?
- How many passwords are likely to be chosen?
- How long will it take to guess?

- Bits of entropy: $\log_2$(# of guesses)

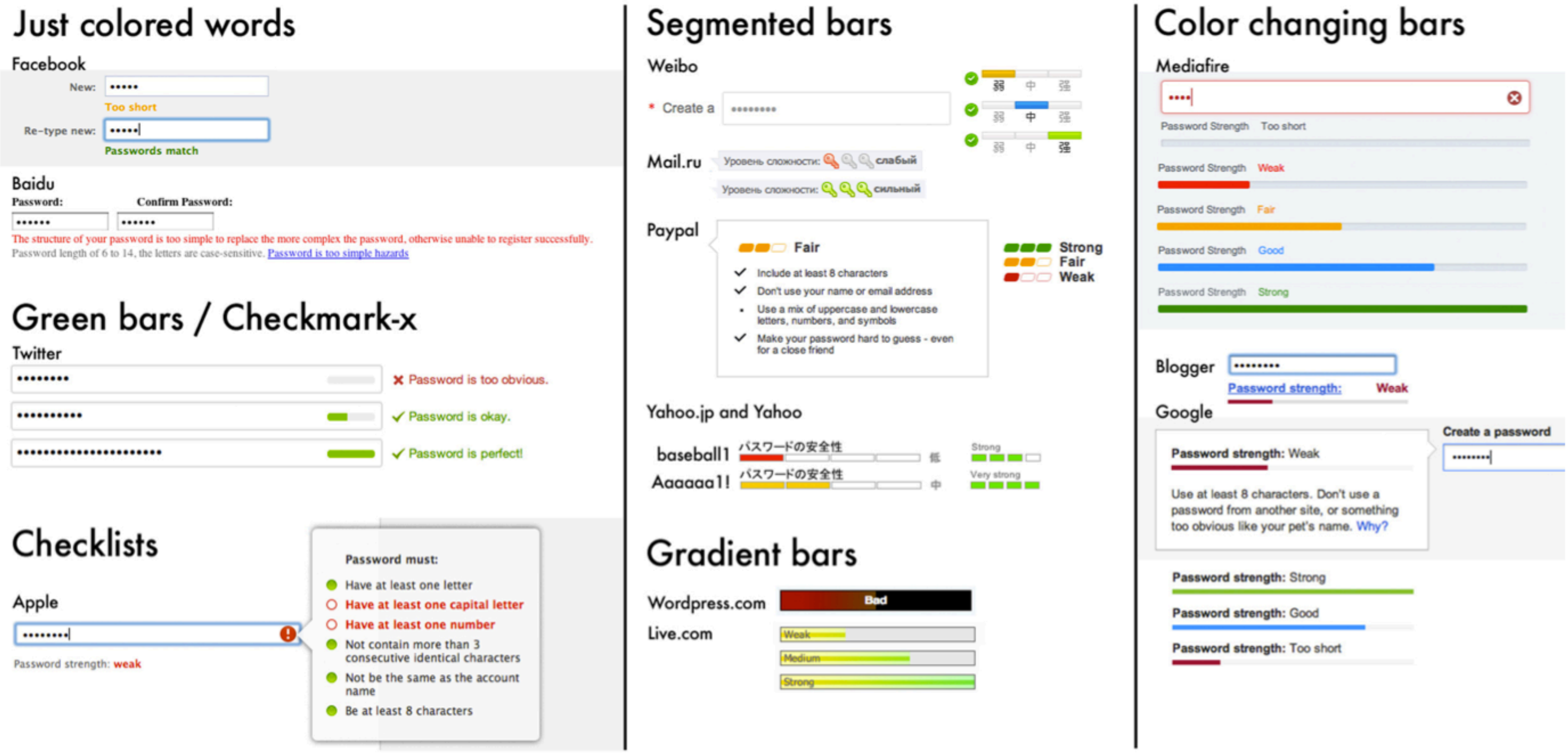
Example: password of 10 bits chosen randomly

Possible passwords = 2^10

Bits of entropy = $\log_2$(2^10) = 10

Additional bit of entropy doubles number of guesses needed.

Password Meters



Just colored words

Facebook

New: ••••••
Too short
Re-type new: ••••••
Passwords match

Baidu

Password: •••••• Confirm Password: ••••••

The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully.
Password length of 6 to 14, the letters are case-sensitive. Password is too simple hazards

Green bars / Checkmark-x

Twitter

•••••••• ✗ Password is too obvious.
••••••••••• ✓ Password is okay.
•••••••••••••••••••••• ✓ Password is perfect!

Checklists

Apple

•••••••• !
Password strength: weak

Password must:
- ● Have at least one letter
- ○ Have at least one capital letter
- ○ Have at least one number
- ● Not contain more than 3 consecutive identical characters
- ● Not be the same as the account name
- ● Be at least 8 characters

Segmented bars

Weibo

* Create a ••••••••
弱 中 强

Mail.ru

Уровень сложности: слабый
Уровень сложности: сильный

Paypal

Fair
- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- • Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Strong
Fair
Weak

Yahoo.jp and Yahoo

baseball1 パスワードの安全性 低 Strong
Aaaaaa1! パスワードの安全性 中 Very strong

Gradient bars

Wordpress.com Bad

Live.com Weak Medium Strong

Color changing bars

Mediafire

••••
Password Strength Too short
Password Strength Weak
Password Strength Fair
Password Strength Good
Password Strength Strong

Blogger ••••••••
Password strength: Weak

Google

Create a password ••••••••
Password strength: Weak
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?

Password strength: Strong
Password strength: Good
Password strength: Too short

[From "How does your password measure up? The Effect of Strength Meters on Password Creation", Ur et al., USENIX Security 2012]

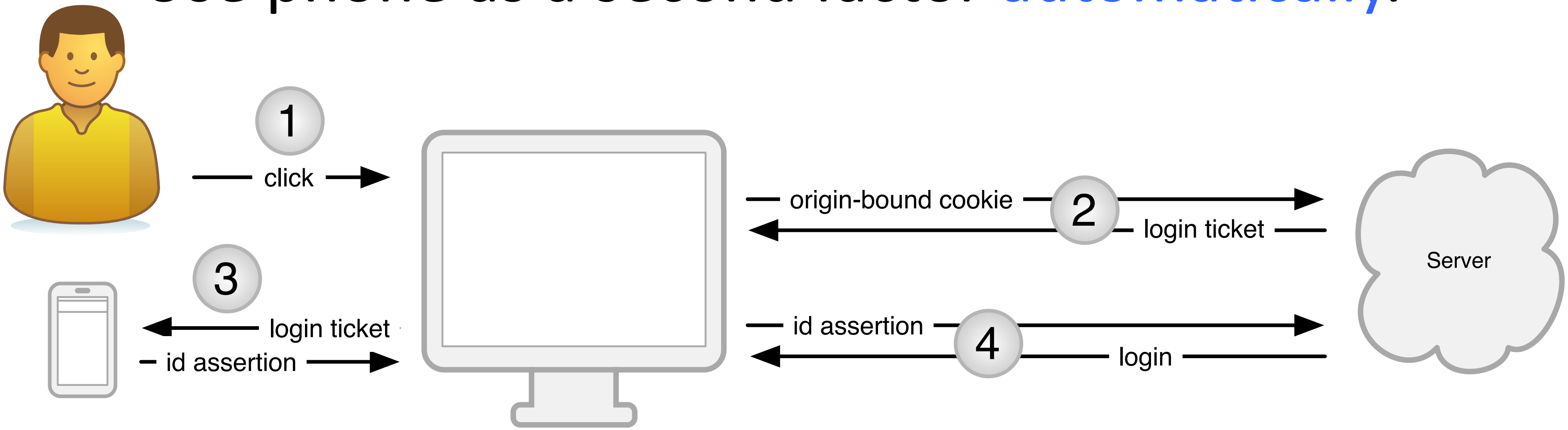
Password Meters

- Meters lead to longer passwords.
- Are passwords harder to guess?
  - Visual feedback alone has no effect.
  - More stringent meters do lead to stronger passwords.
- Meters lead to people taking longer to create passwords, and change their mind during creation.
- Meters don’t affect memorability.

[From “How does your password measure up? The Effect of Strength Meters on Password Creation”, Ur et al., USENIX Security 2012]

Usable Two-Factor Authentication

- Use phone as a second factor automatically.



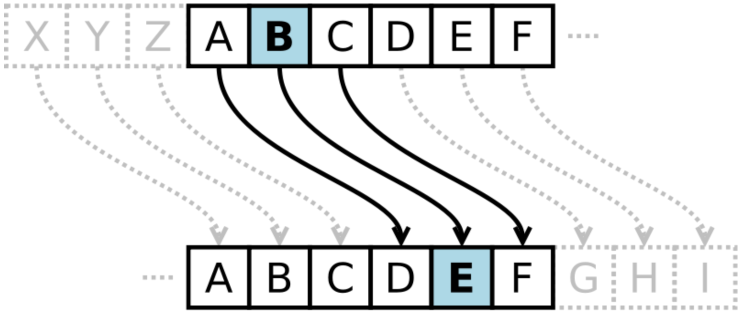
- What if phone is not present?
  - Server can treat login session differently (e.g., don’t allow transactions above a threshold $ amount).

[From “Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions”, Czeskis et al., CCS 2012]

Cryptography

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)

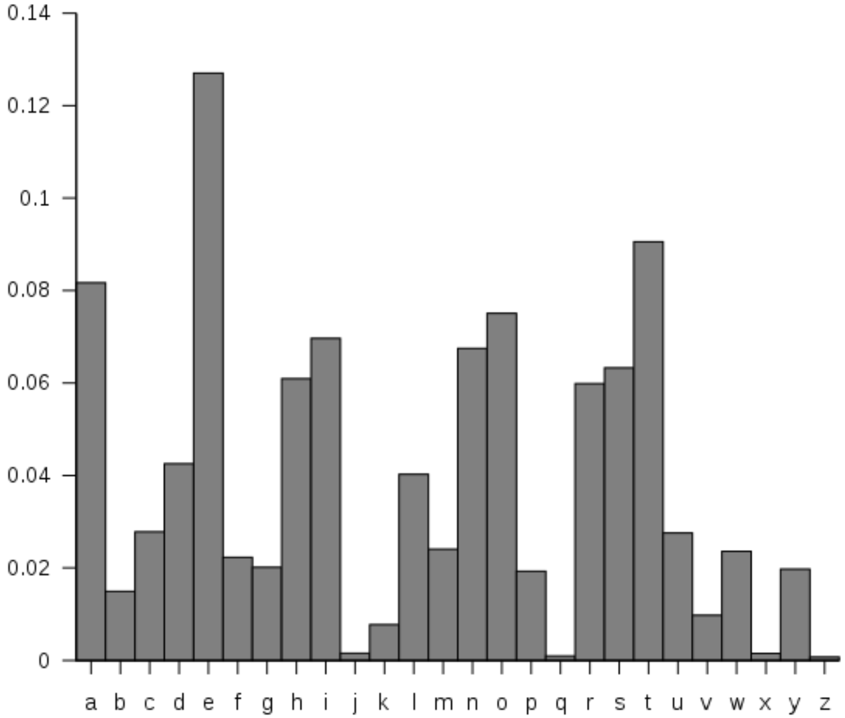
- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.

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

Transposition Cipher

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

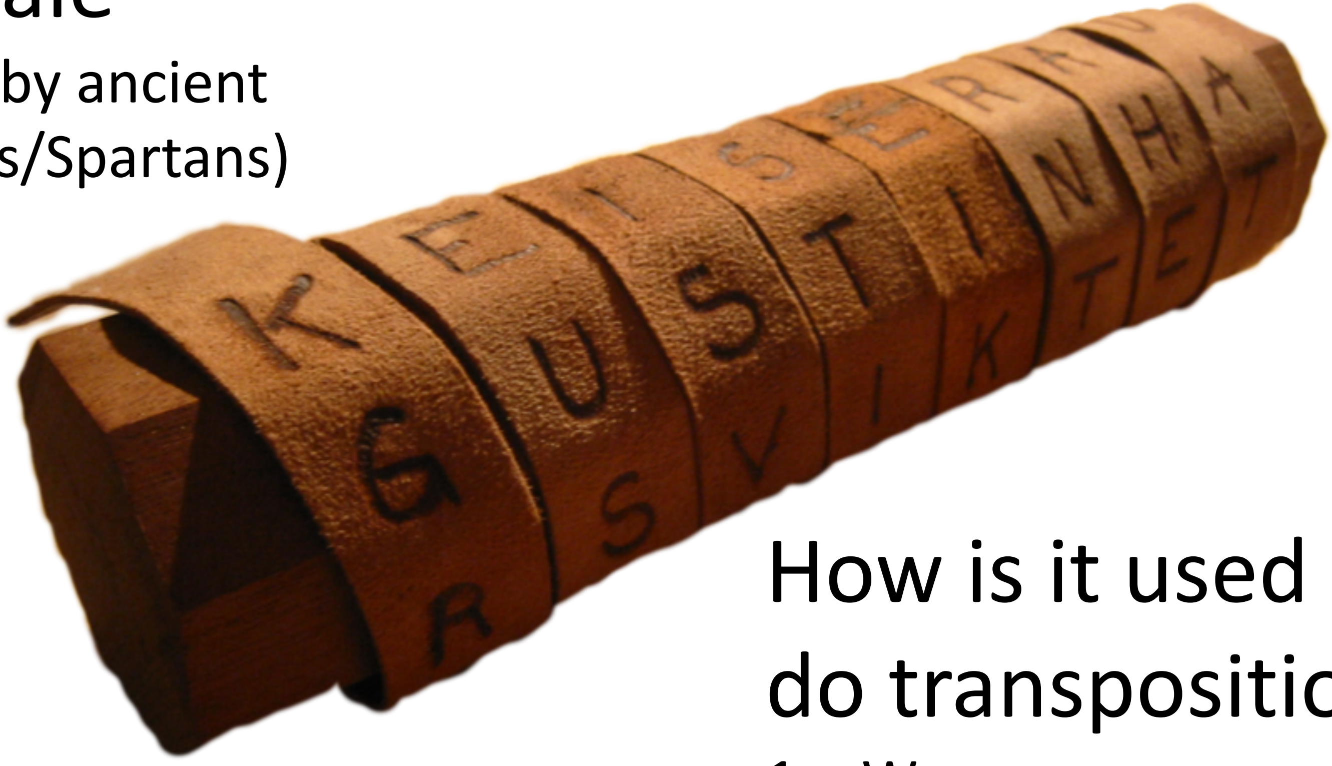
W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

  - 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?

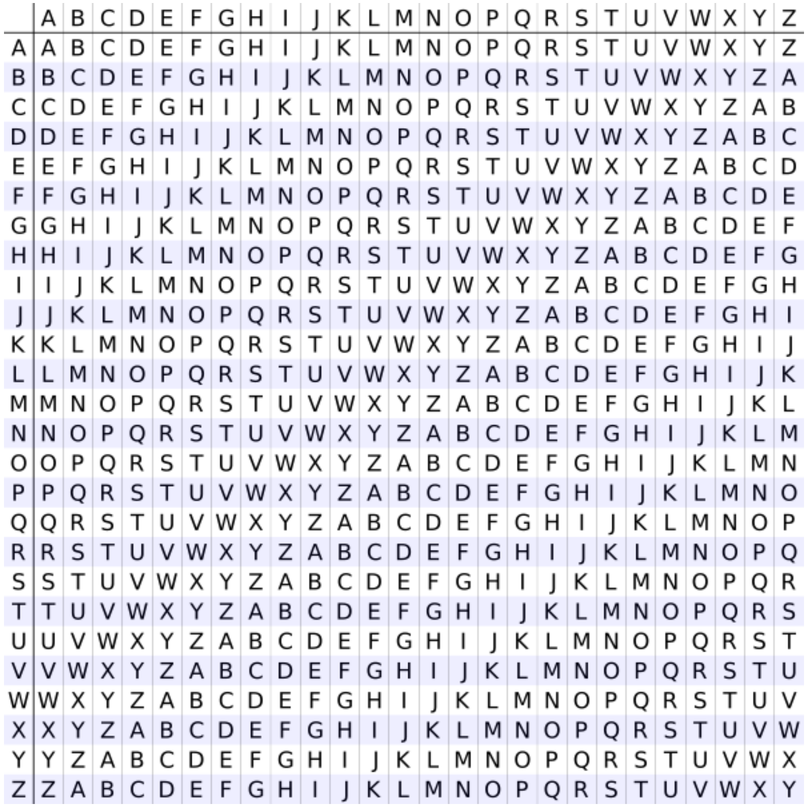
1. Wrap
2. Write horizontally
3. Encrypt = unwrap
4. Decrypt = rewrap

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 5th 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…)

Steganography

- Hidden messages (security through obscurity)

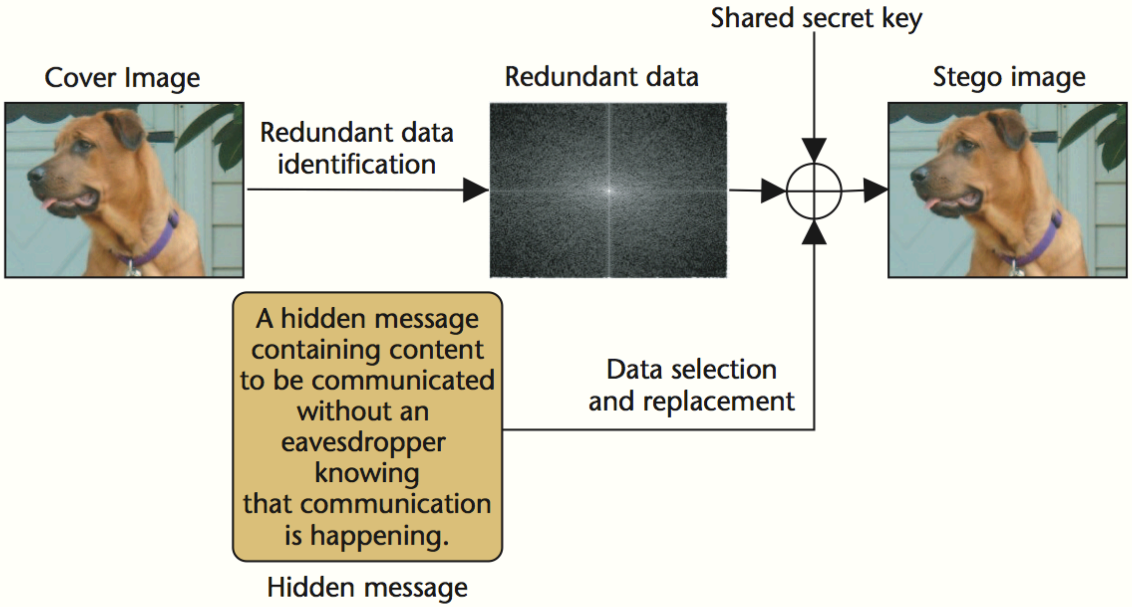
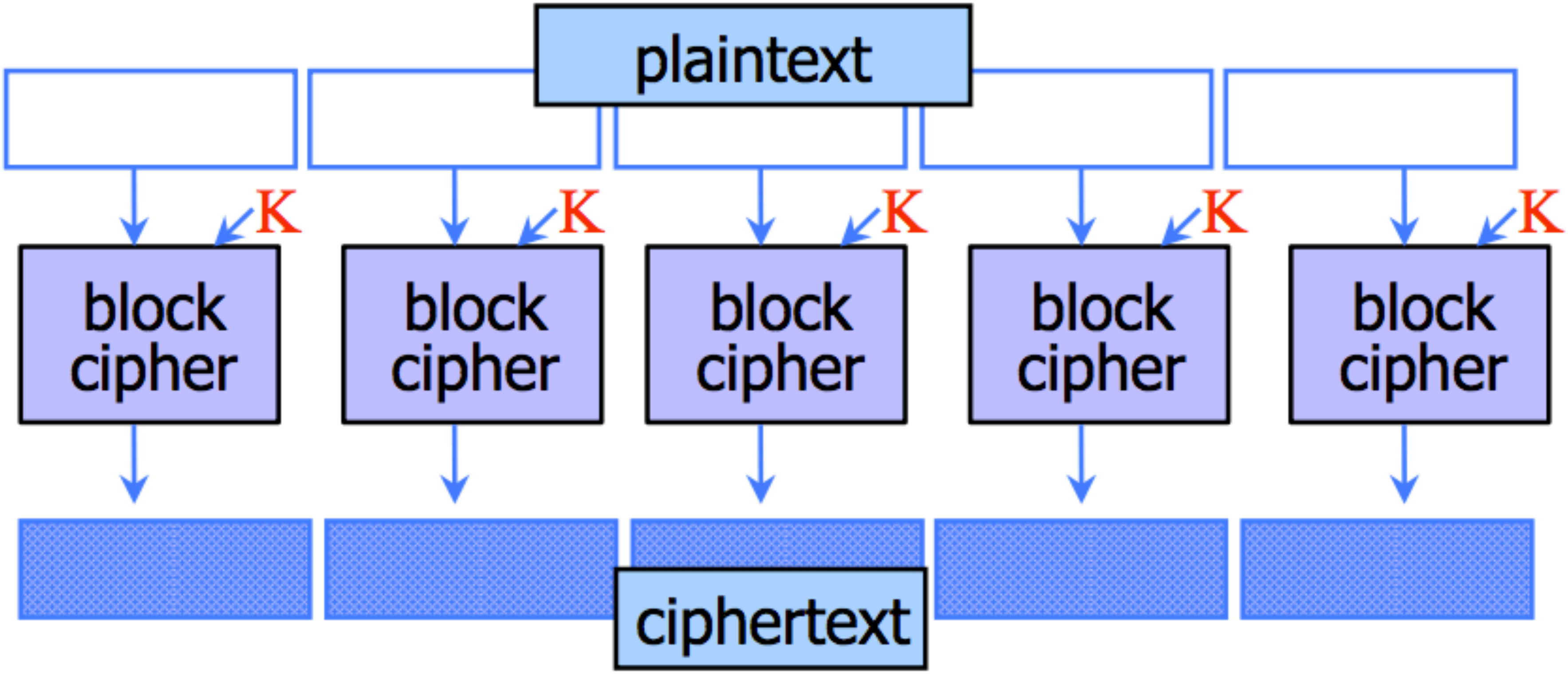

Shared secret key
Cover Image
Redundant data
Stego image
Redundant data identification
A hidden message containing content to be communicated without an eavesdropper knowing that communication is happening.
Data selection and replacement
Hidden message

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.

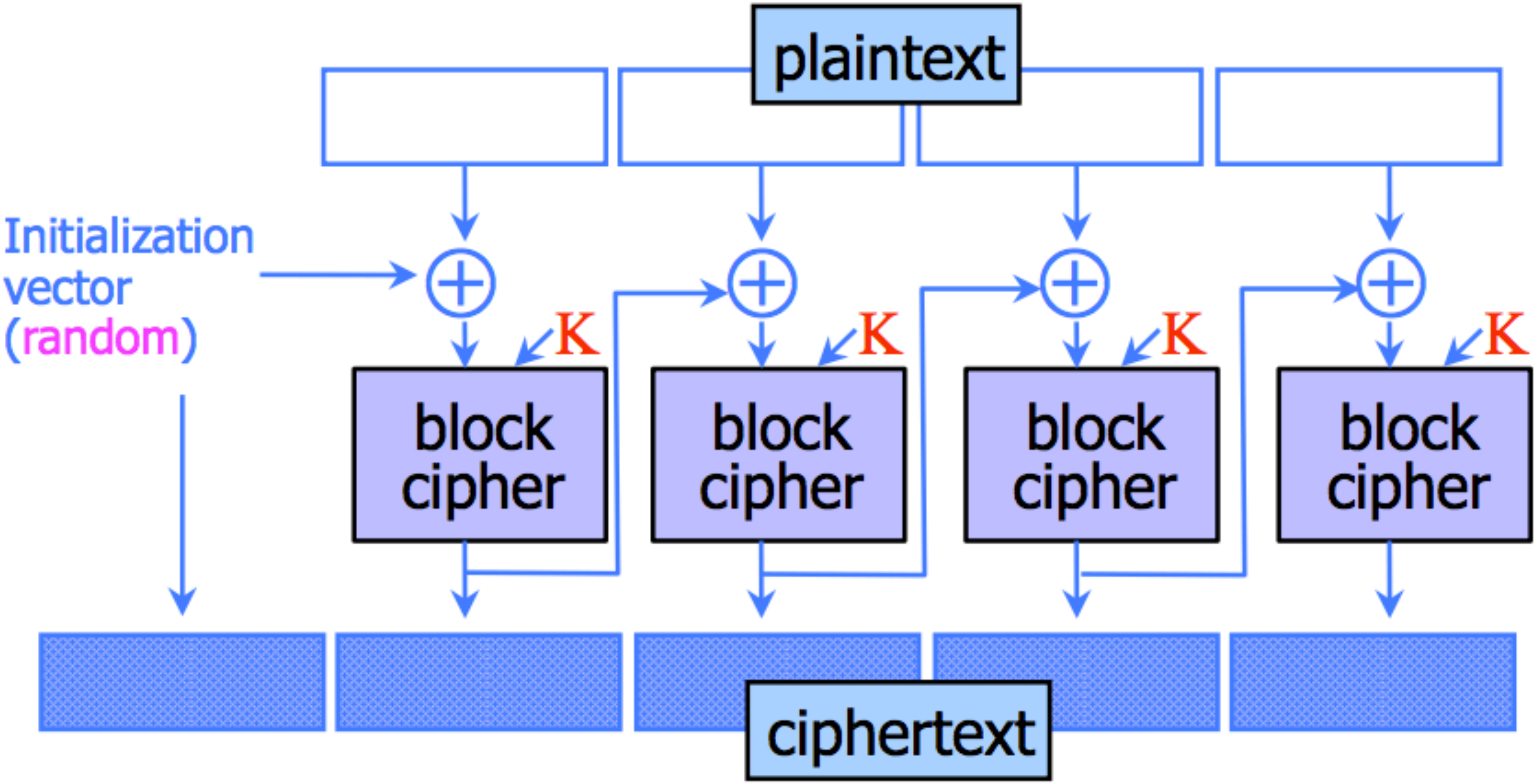
[Figure from "Hide and Seek: An Introduction to Steganography" by Niels Provos and Peter Honeyman]

Block Cipher Mode: ECB



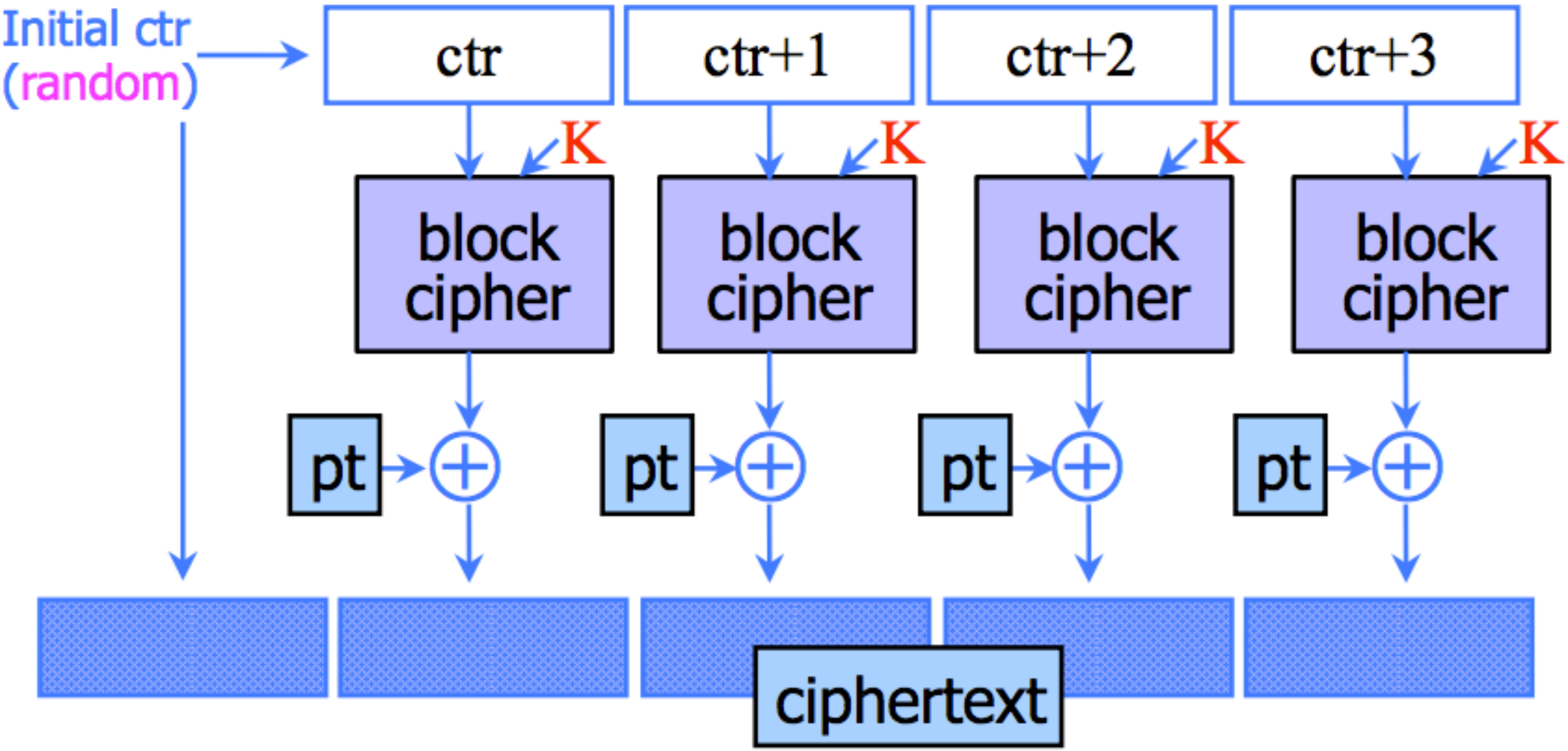
[Figure from Yoshi's slides]

Block Cipher Mode: CBC



[Figure from Yoshi's slides]

Block Cipher Mode: CTR



[Figure from Yoshi's slides]