CSE 484 / CSE M 584

Computer Security Section Week 4: Cryptography

TA: Thomas Crosley
tcrosley@cs

Thanks to Franzi Roesner and Adrian Sham for previous slides

[Examples/Images thanks to Wikipedia.]

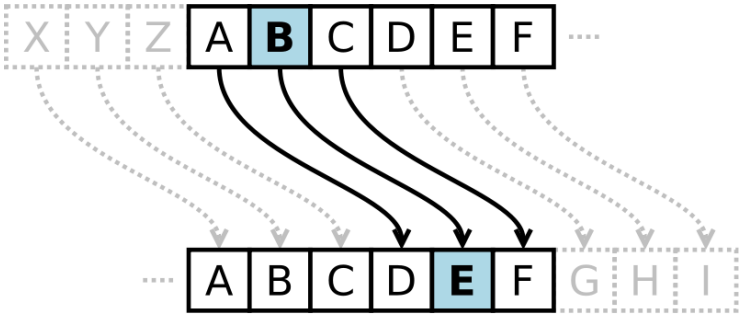
Administrivia

- Lab 1 Final due next week (Friday 4/29, 8pm)
- Today
  - Fun Historical Ciphers
  - Crypto Review
  - Crypto Practice
  - CBC-MAC Issue

Fun Historical Ciphers

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)

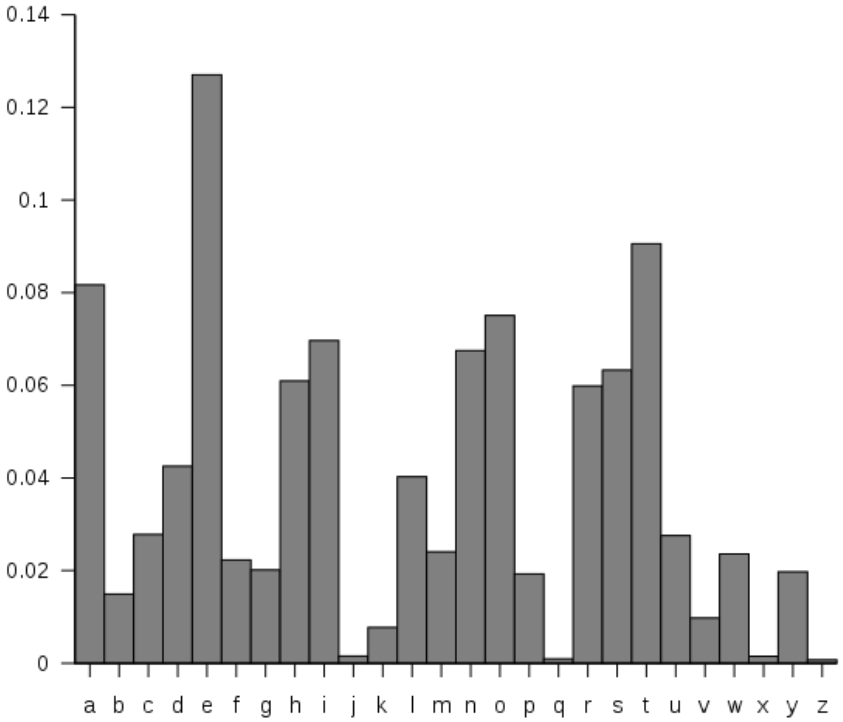
- ROT13: shift 13 (encryption and decryption are symmetric)
- What is the key space?
  - 26 possible shifts.
- How to attack shift ciphers?
  - Brute force.

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

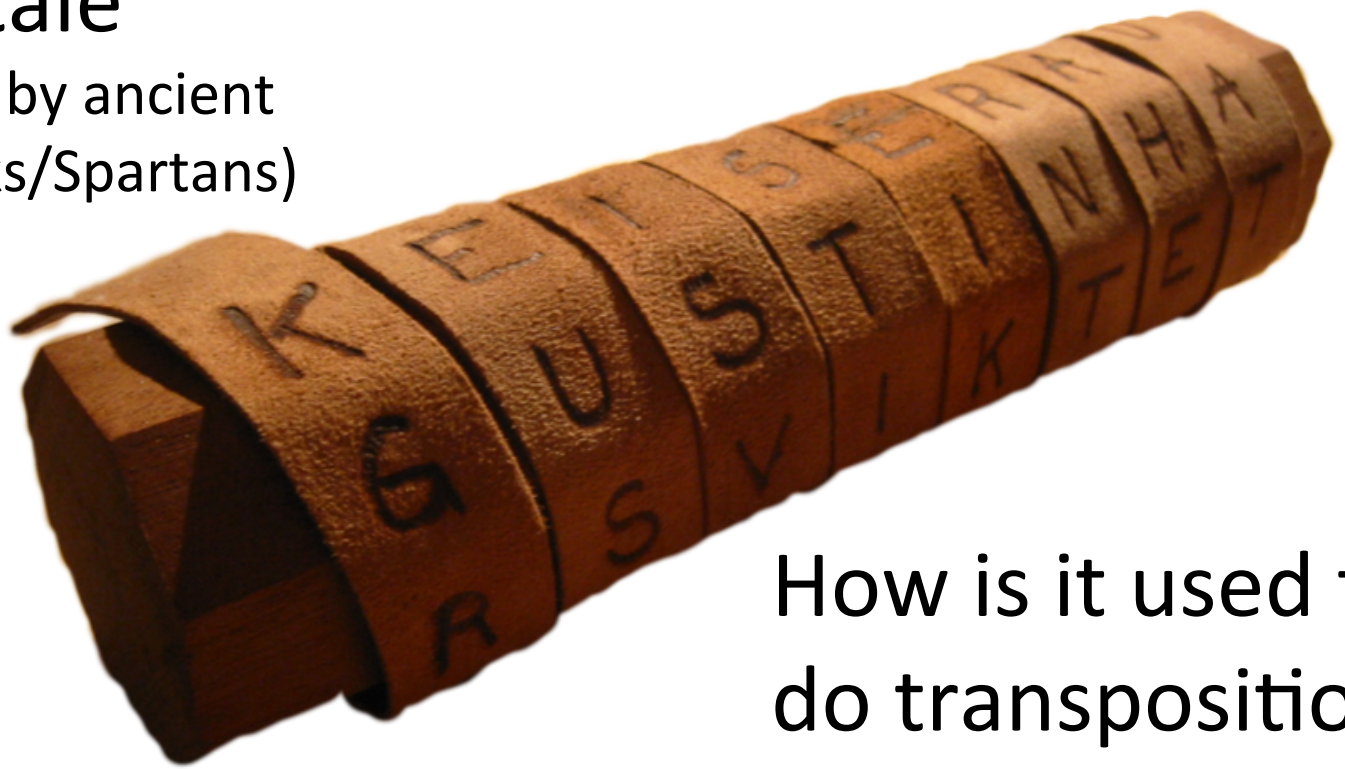
- Ciphertext is permutation of plaintext.
- Example: **Route cipher**
  - Plaintext: `WE ARE DISCOVERED, FLEE AT ONCE`
  - Arrangement:

    ```
    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?

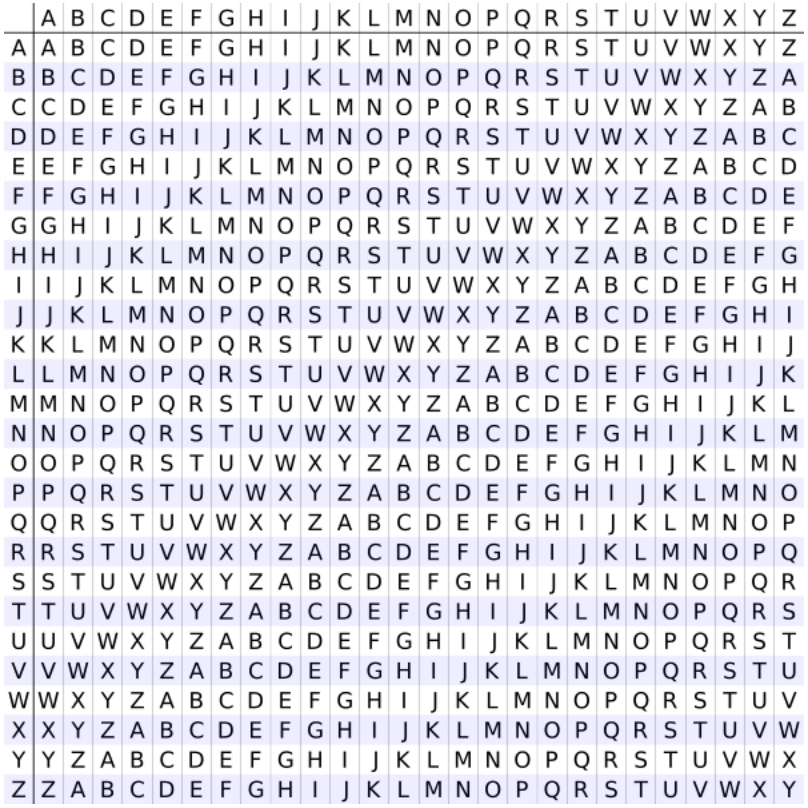
1. Wrap
2. Write horizontally
3. Encrypt = unwrap
4. Decrypt = rewrap

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



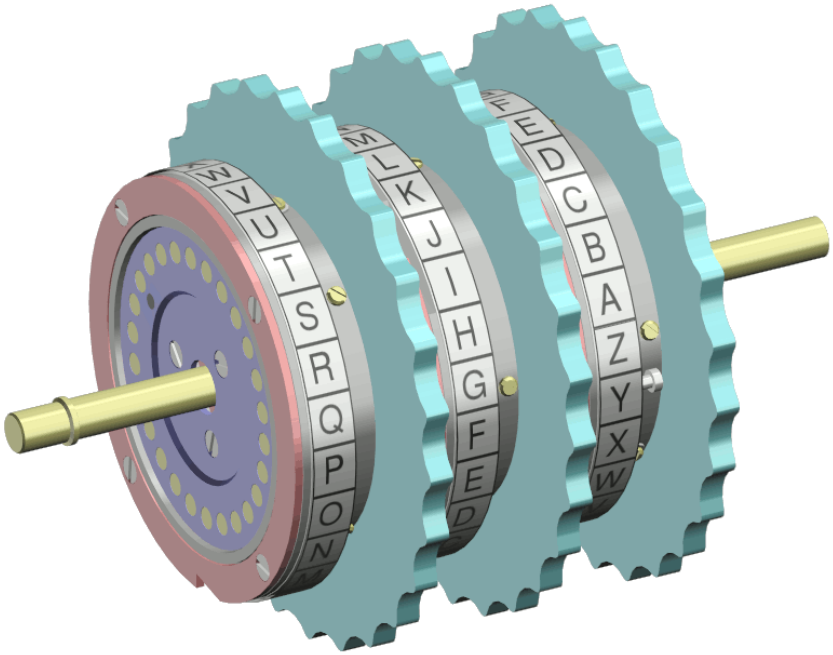
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

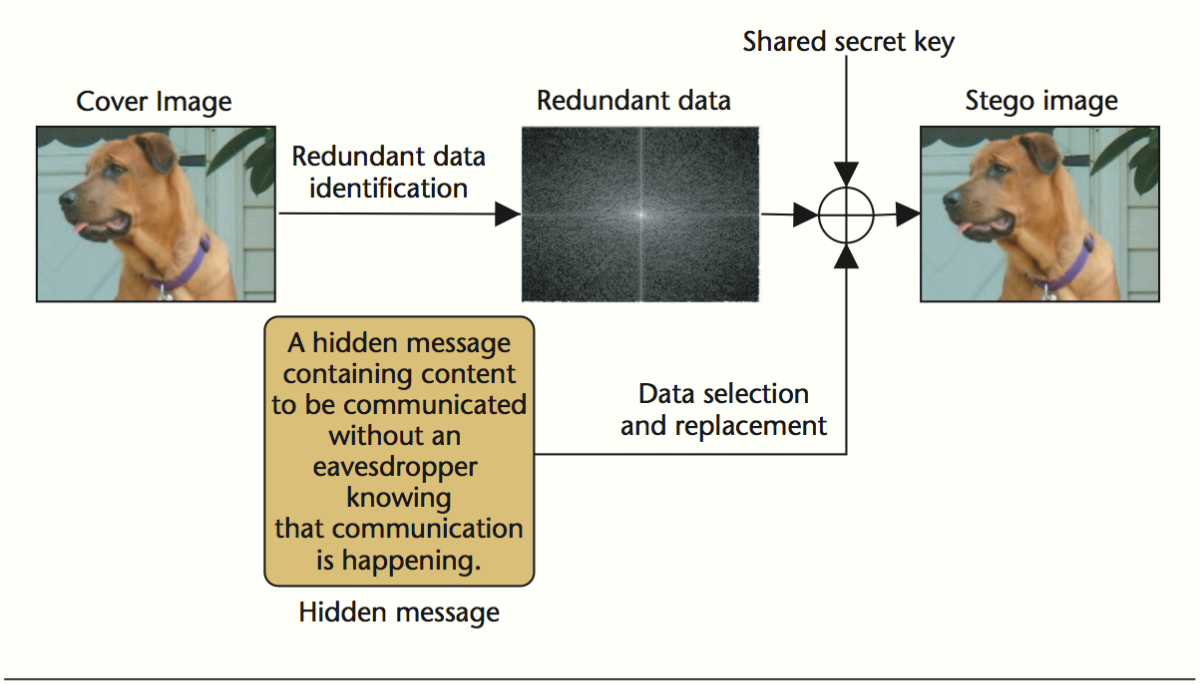


Figure 1. Modern steganographic communication. The encoding step of a steganographic system identifies redundant bits and then replaces a subset of them with data from a secret message.

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

Secret Messages in Video Games

- *Castle*: program that encodes secret messages in video game communications
  - Stony Brook University
  - Avoiding surveillance and firewalls in China
  - Still looks like a normal game from the outside
- Encode: message -> player movements
- Decode: player movements -> message

Source: http://www.wired.com/2015/04/app-hides-secret-messages-starcraft-style-games/

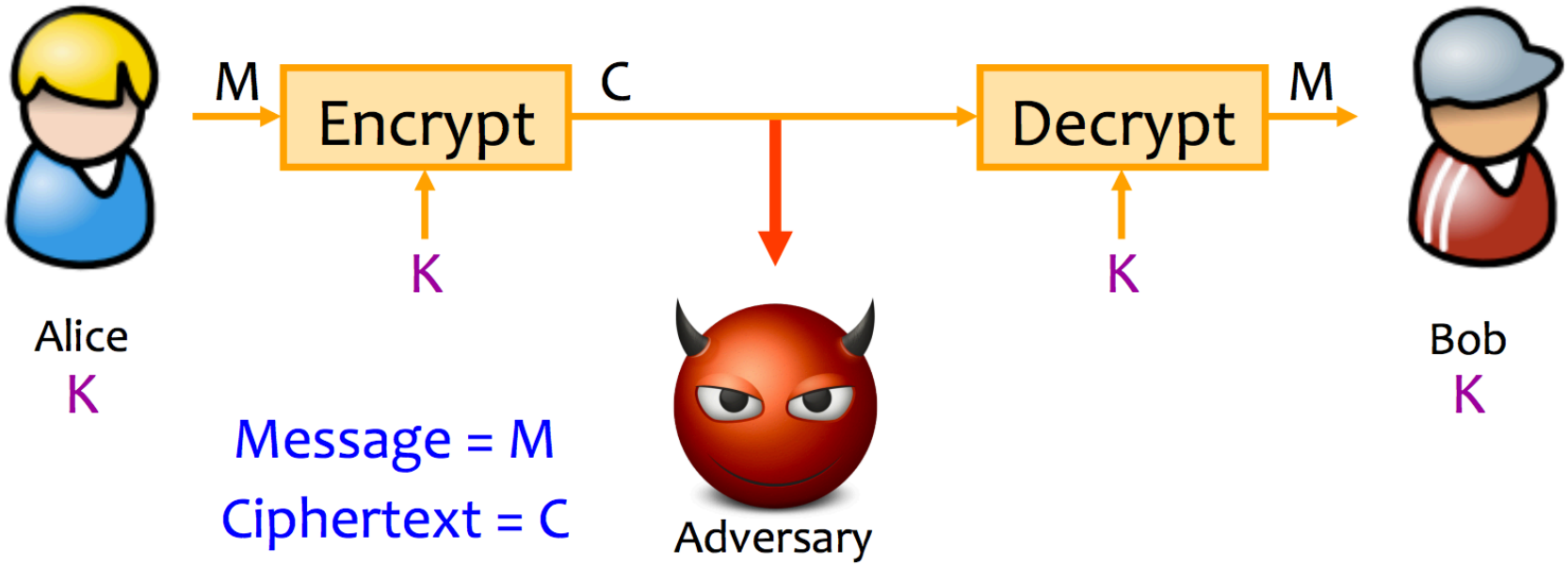
Crypto Review

Flavors of Cryptography

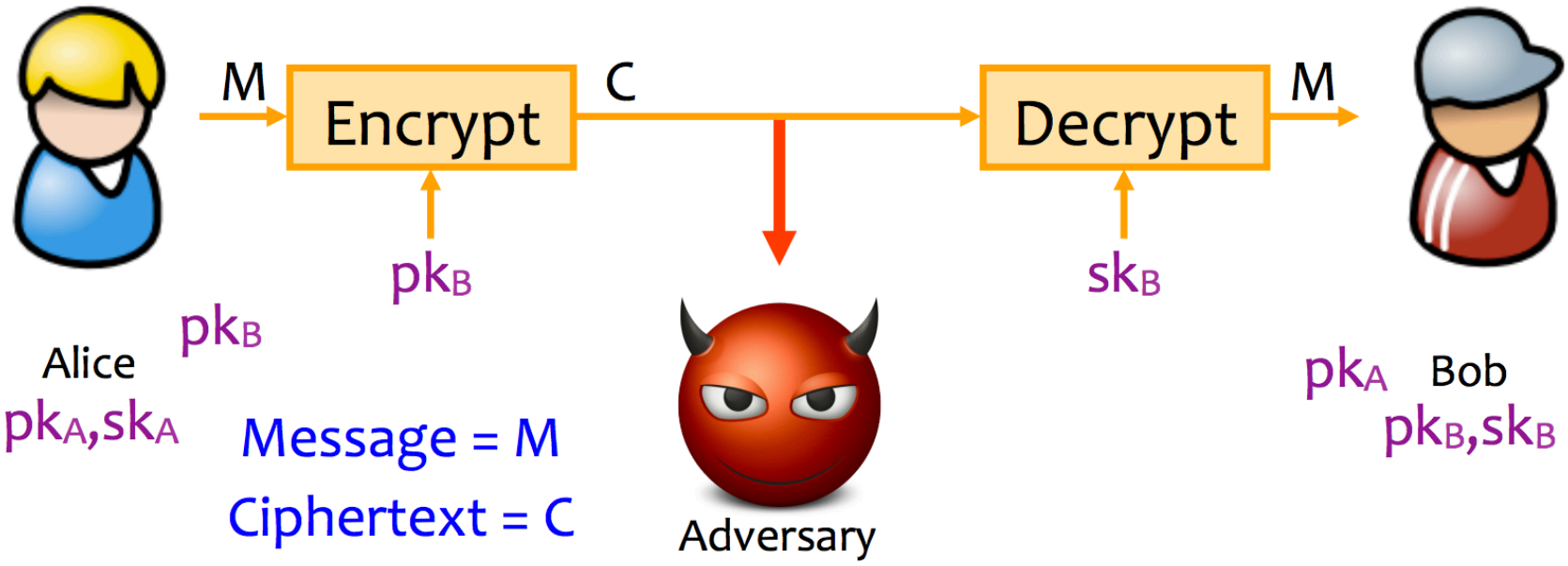
- Symmetric cryptography
  - Both communicating parties have access to a **shared random string** K, called the key.

- Asymmetric cryptography
  - Each party creates a public key pk and a secret key sk.

Achieving Privacy (Symmetric)

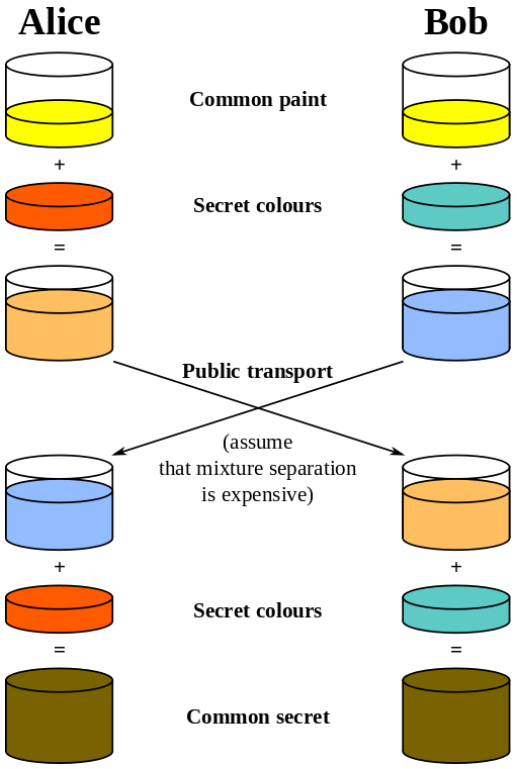


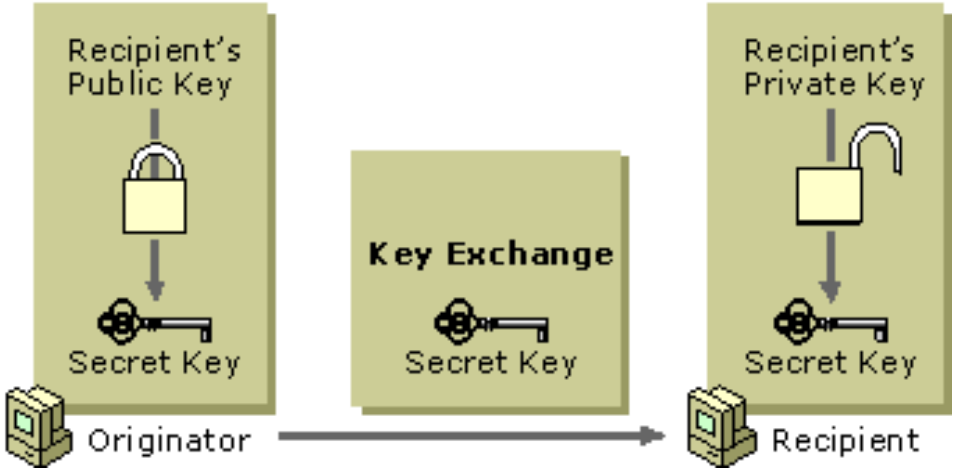
Achieving Privacy (Asymmetric)



Key exchange

- Diffie-Hellman Key Agreement algorithm
- RSA key exchange process (Next week!)

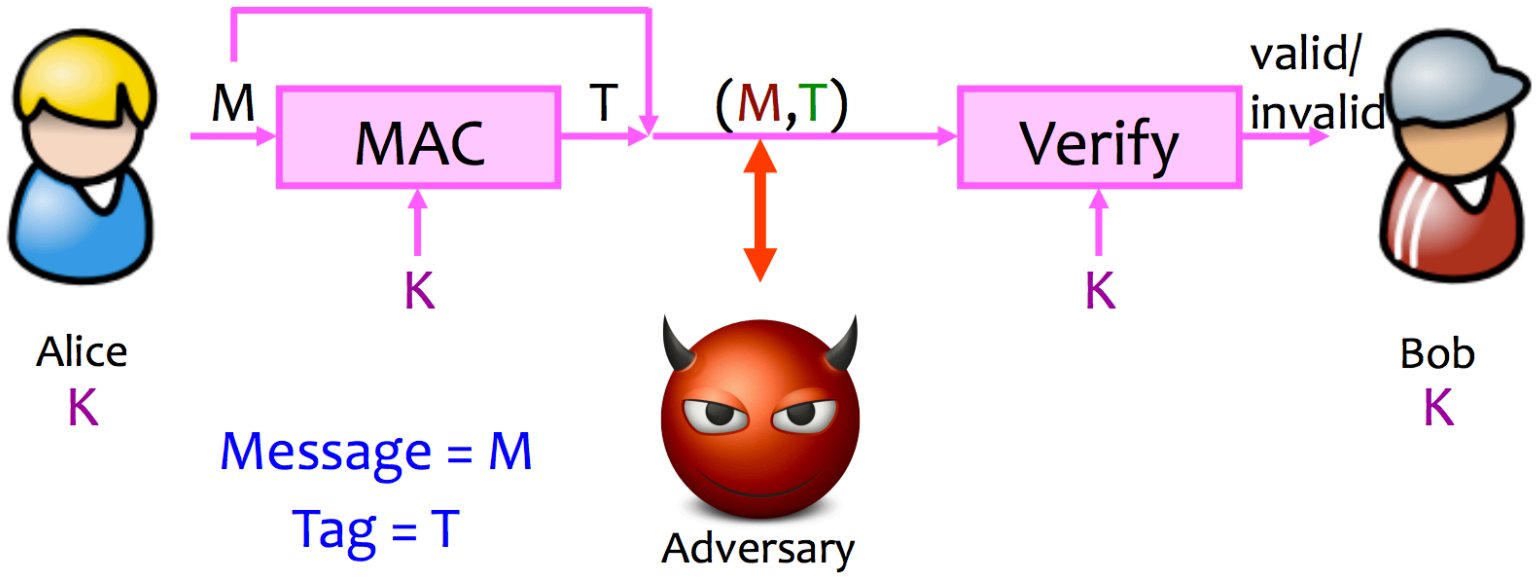




https://technet.microsoft.com/en-us/library/cc962035.aspx

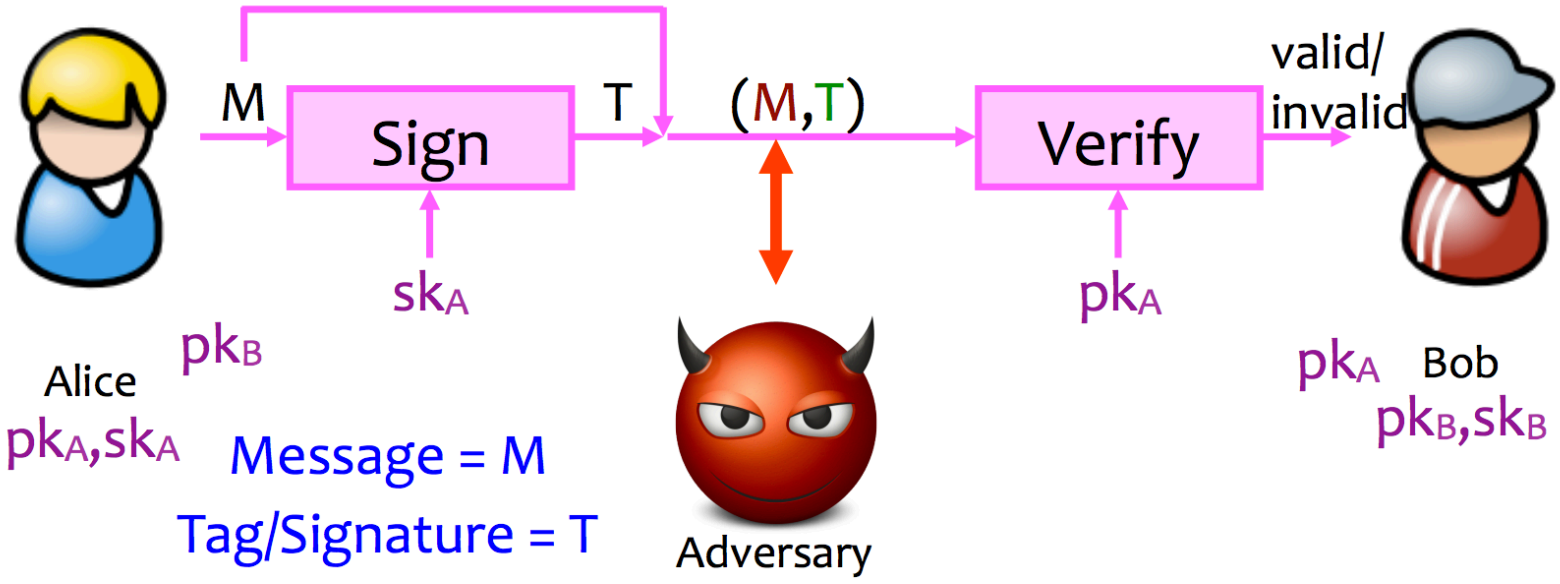
Achieving Integrity (Symmetric)

- Message authentication schemes: A tool for protecting integrity. (Also called message authentication codes or MACs)



Achieving Integrity (Asymmetric)

Digital signature schemes: A tool for protecting integrity and authenticity.



Pseudo Random Number Generator (PRNG)

- Algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.
- In other word, sort of random, but not REALLY…

Crypto Practice

Diffie-Helman Protocol

- Alice and Bob never meet and share no secret
- Public info: p and g
  - P is a large prime (public info)
  - G is a generator (public info)
- Alice sends -> Bob $g^x \bmod p$
- Bob sends -> Alice $g^y \bmod p$
- $k = (g^x)^y = (g^y)^x = g^{xy} \bmod p$ (shared secret)

Diffie Helman Practice Problem

- P = 11
- G = 7
- Alice's Private Key (x = 4)
- Bob's Private Key (y = 8)

- What is their shared key?

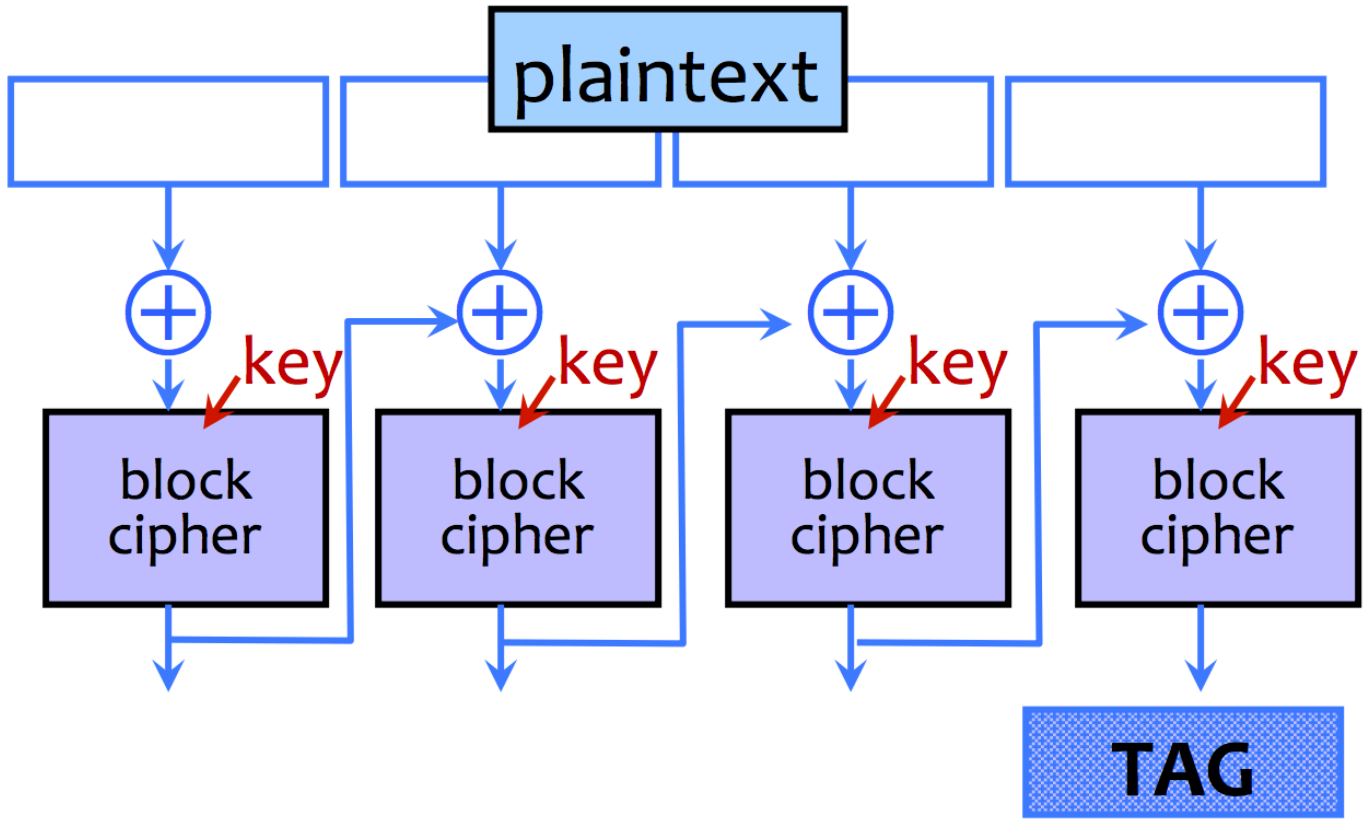
Practice Problem Solution

- Alice computes $7^4 \bmod 11 = 3$
- Bob computes $7^8 \bmod 11 = 9$
- Shared secret is $3^8 = 9^4 \bmod 11 = 5$

CBC-MAC Problem

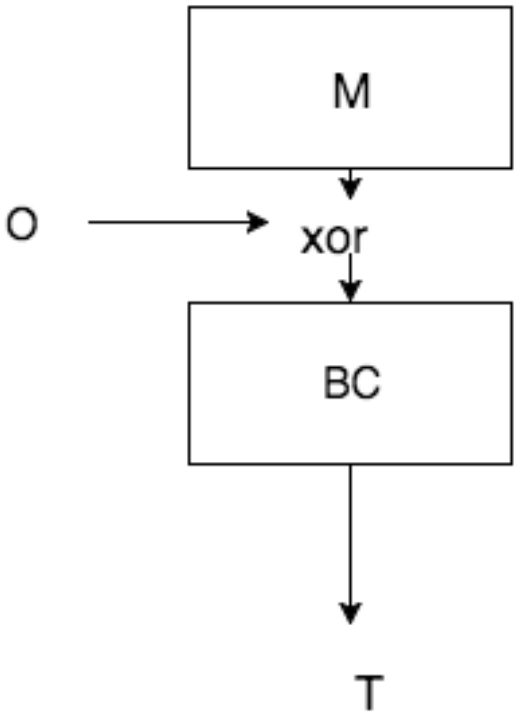
Integrity does not work here with variable length messages

CBC-MAC


plaintext
key
key
key
key
block cipher
block cipher
block cipher
block cipher
TAG

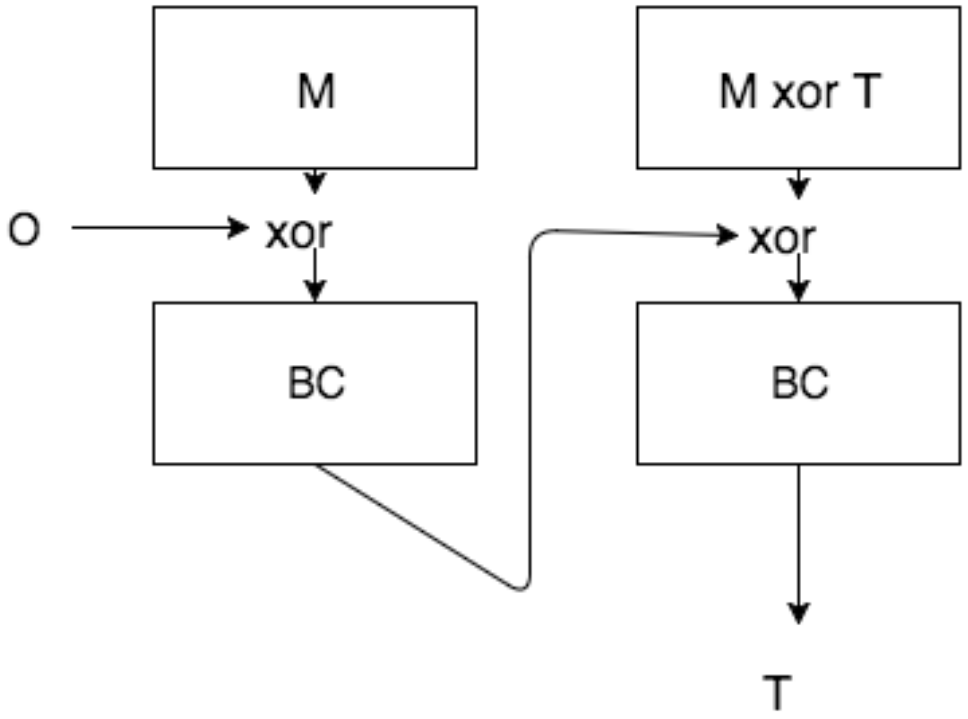
CBC-MAC Problem

One Block Message (M)



BC(M xor O) = T

Forgery: 2 Blocks, M and M xor T



BC(BC(M xor O) xor (M xor T))
= BC(T xor M xor T) = B(M) = T