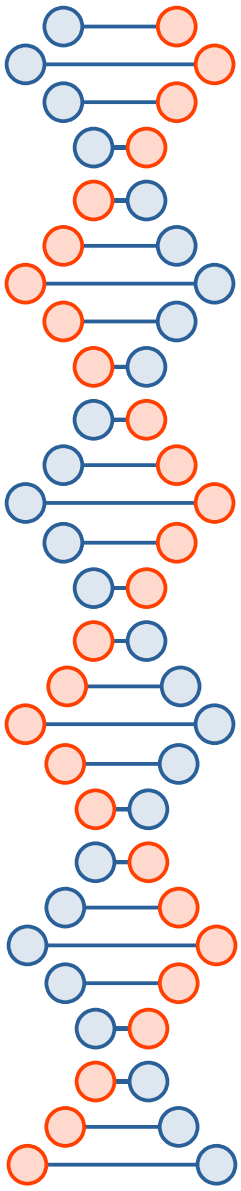
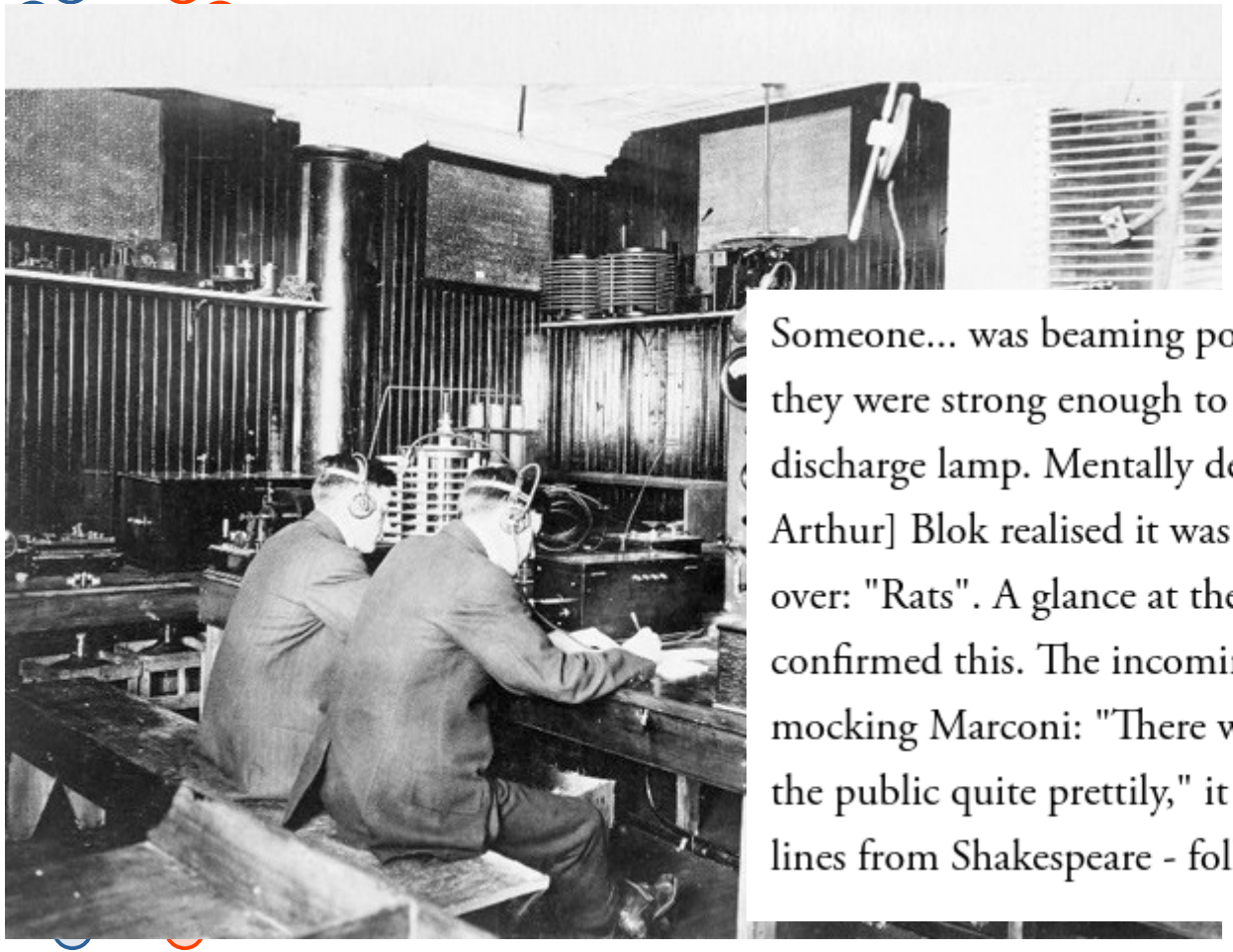


Symmetric Cryptography (Through the 1980s or so…) and Diffie-Hellman

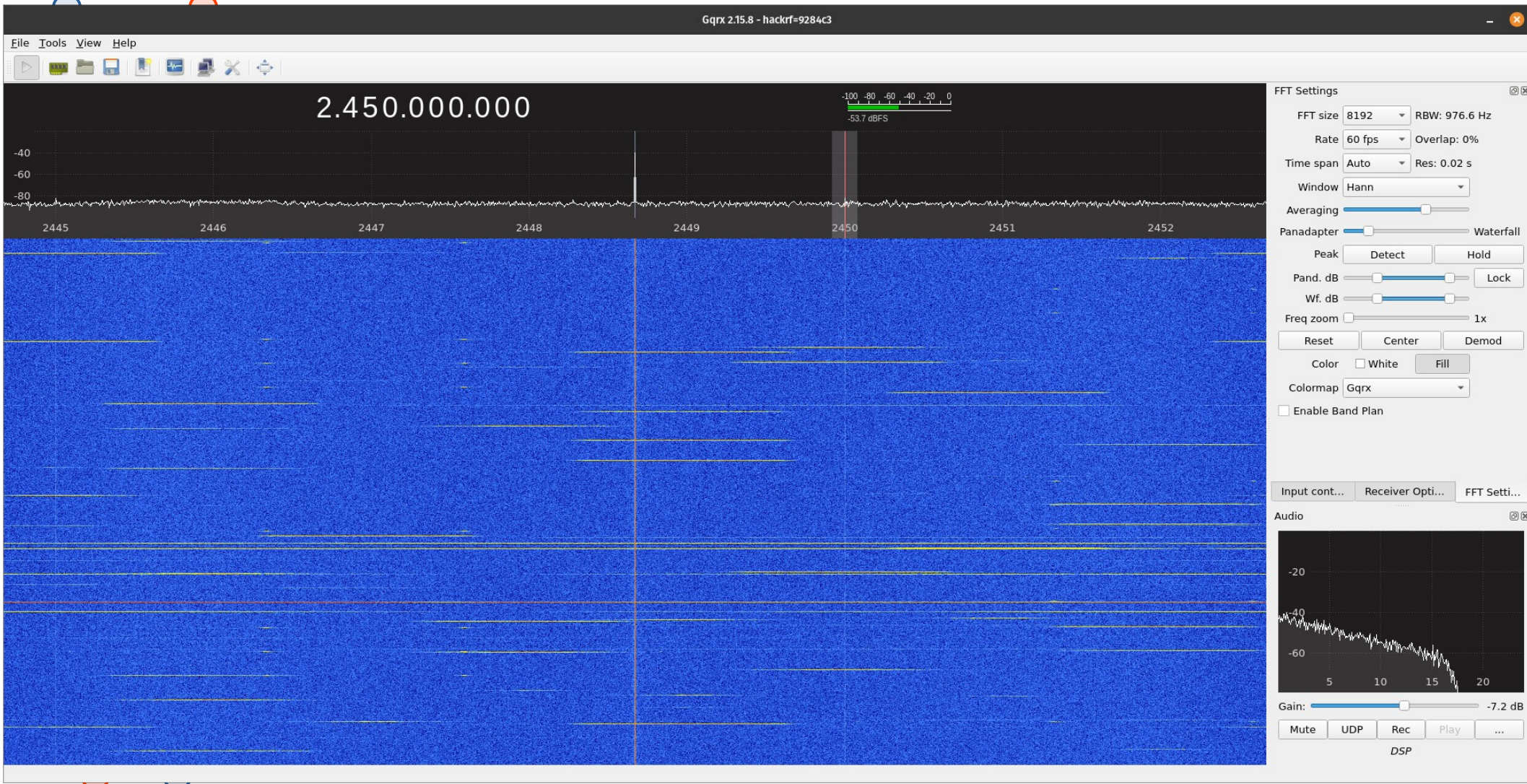
CSE 548 Fall 2025

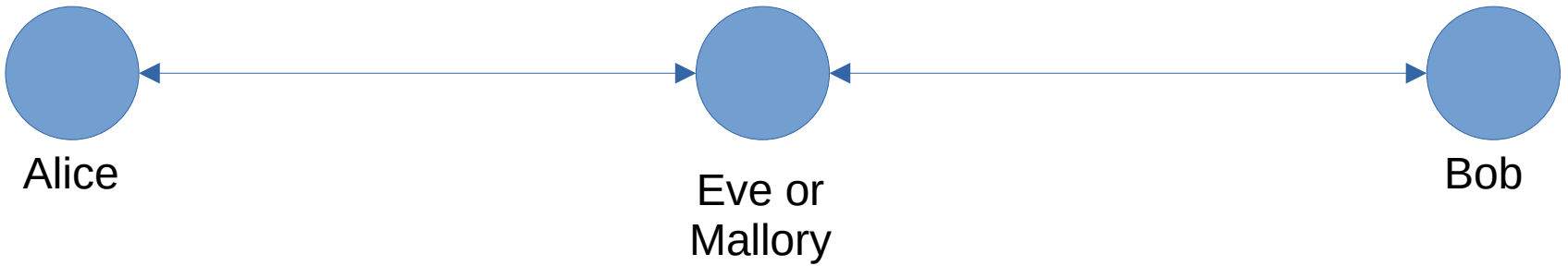
jedimaestro@asu.edu

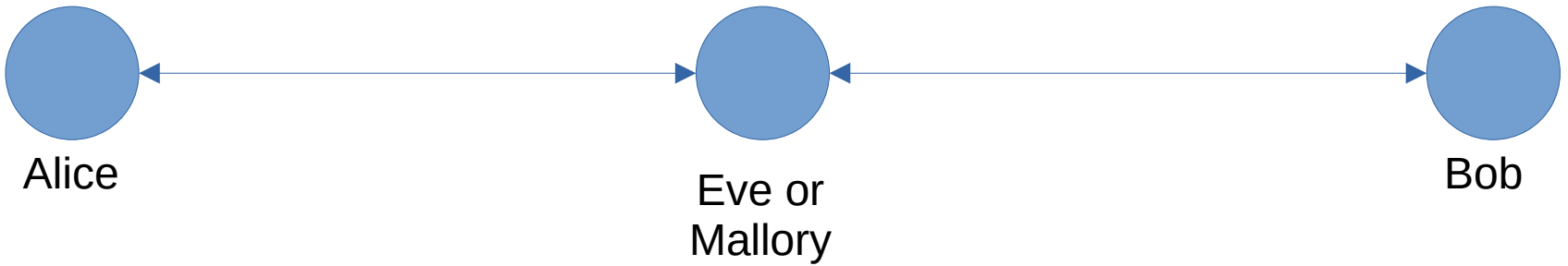


Someone... was beaming powerful wireless pulses into the theatre and they were strong enough to interfere with the projector's electric arc discharge lamp. Mentally decoding the missive, [Fleming's assistant Arthur] Blok realised it was spelling one facetious word, over and over: "Rats". A glance at the output of the nearby Morse printer confirmed this. The incoming Morse then got more personal, mocking Marconi: "There was a young fellow of Italy, who diddled the public quite prettily," it trilled. Further rude epithets - apposite lines from Shakespeare - followed.

https://www.theatlantic.com/technology/archive/2011/12/the-great-wireless-hack-of-1903/250665/


Gqrx 2.15.8 - hackrf=9284c3
File Tools View Help
2.450.000.000
-100 -80 -60 -40 -20 0
-53.7 dBFS
-40
-60
-80
2445
2446
2447
2448
2449
2450
2451
2452
FFT Settings
FFT size 8192
RBW: 976.6 Hz
Rate 60 fps
Overlap: 0%
Time span Auto
Res: 0.02 s
Window Hann
Averaging
Panadapter
Waterfall
Peak
Detect
Hold
Pand. dB
Lock
Wf. dB
Freq zoom
1x
Reset
Center
Demod
Color
White
Fill
Colormap Gqrx
Enable Band Plan
Input cont...
Receiver Opti...
FFT Setti...
Audio
-20
-40
-60
5
10
15
20
Gain:
-7.2 dB
Mute
UDP
Rec
Play
...
DSP

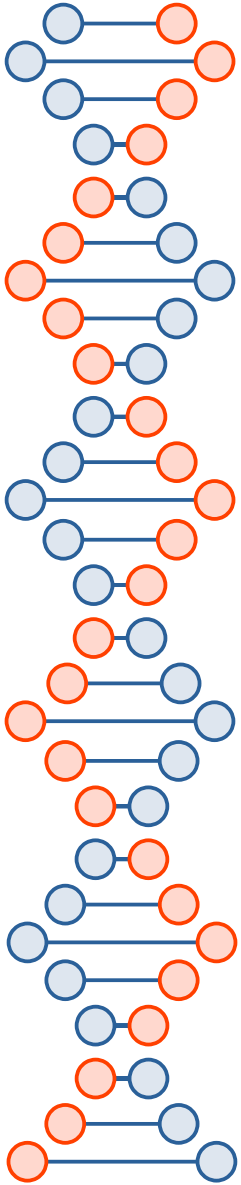

Alice
Eve or
Mallory
Bob



WiFi, electric path, or optical… Eve or Mallory get their own copy!

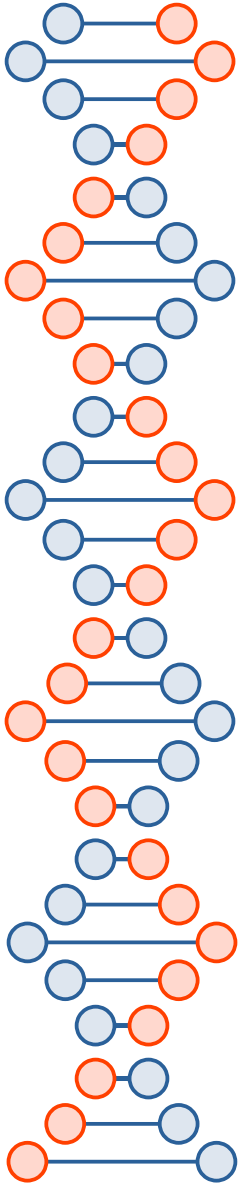
Alternatives to crypto

- Code division multiple access (CDMA)
  - Invented (in the U.S., at least) by Hedy Lamarr
- Information theory, randomized algorithms, *etc.*
  - Currently not practical in terms of solving all our problems
- Line-of-sight, directional antennae
  - Not entirely practical for security reasons, but increasingly common for other reasons
  - Line of sight attacker (*e.g.*, drone or in the Internet backbone)



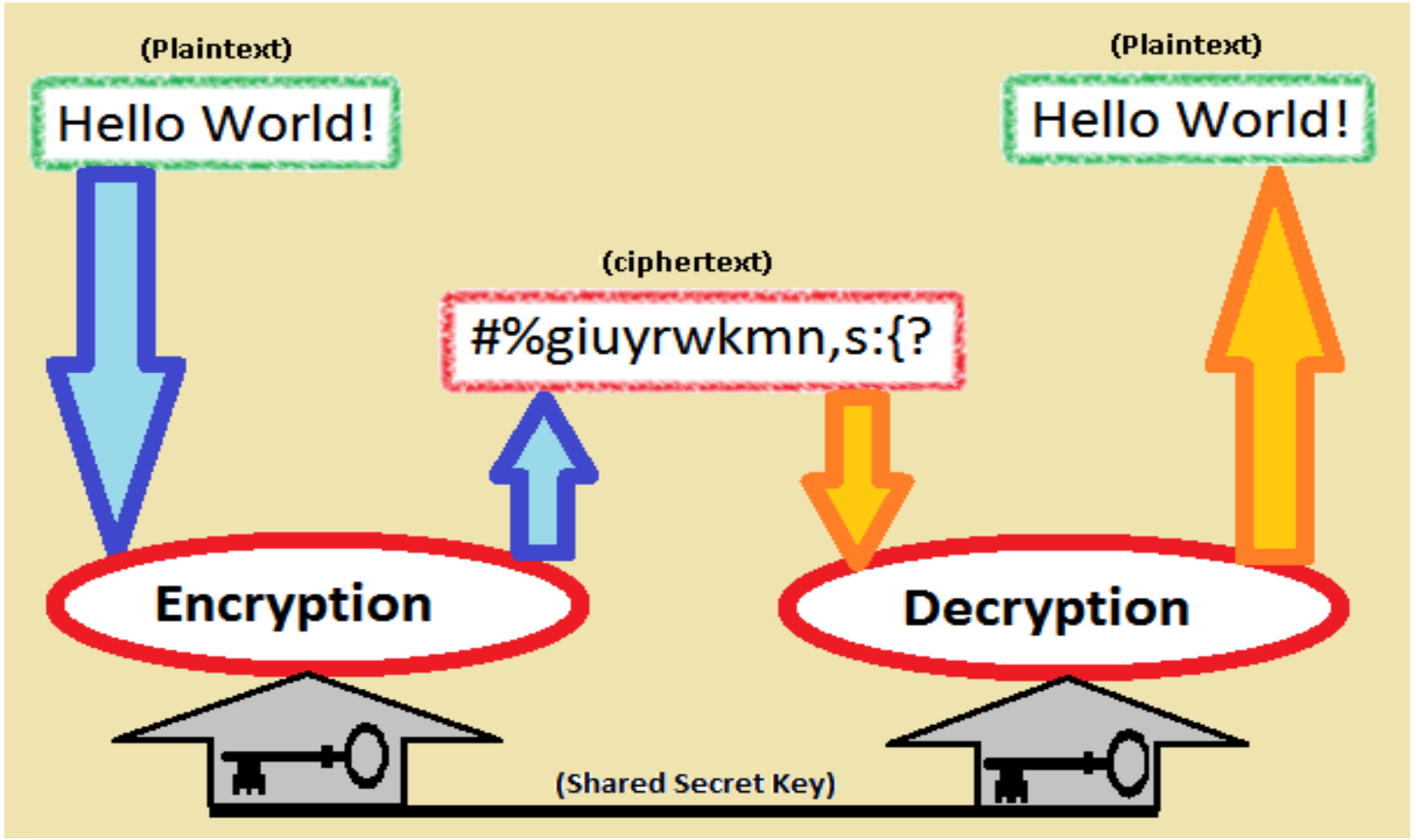
Basics of crypto...

- 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)
  - Quantum computers break current algorithms that are used in practice
- Secure hash functions and message authentication

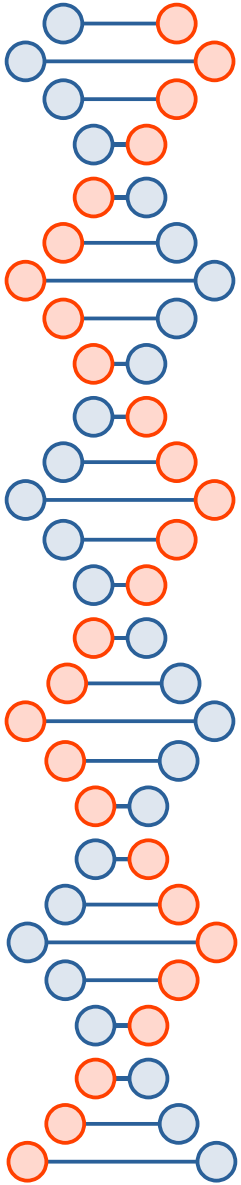


Symmetric Crypto

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

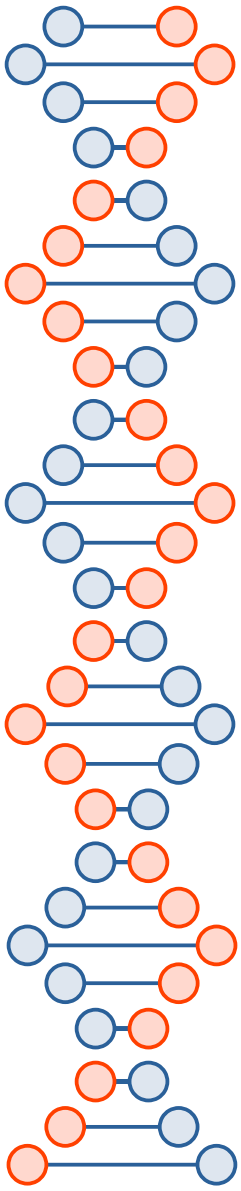


Source: Wikipedia



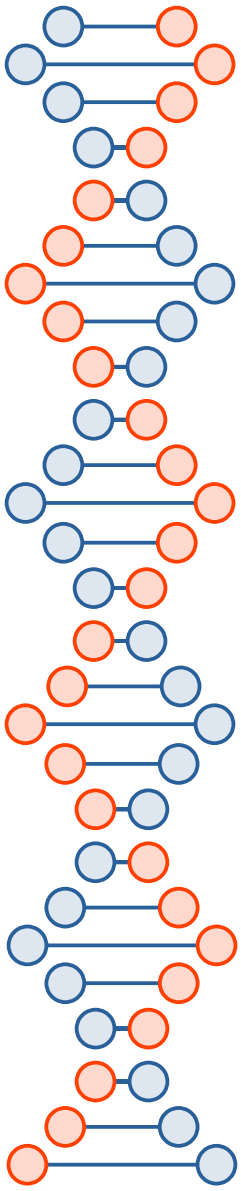
Terminology

- 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



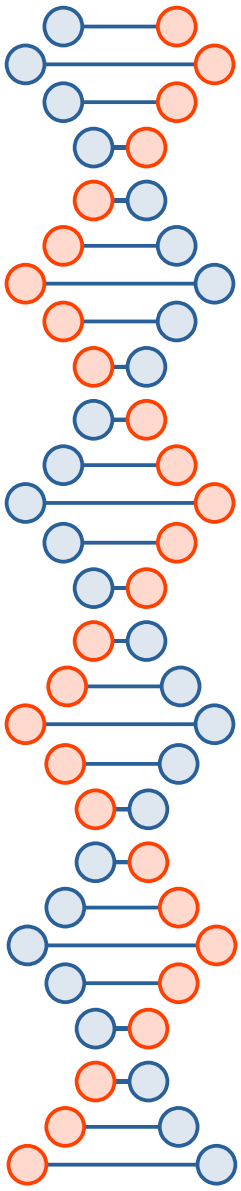
Review on your own...

- Caesar Cipher
- Vigenere Cipher and related attacks



Modern symmetric crypto

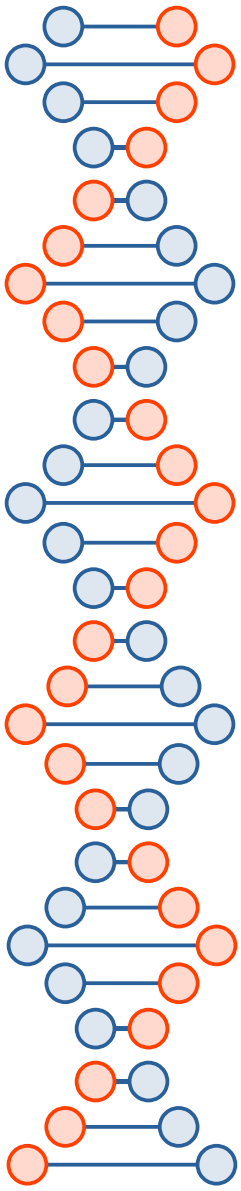
- Mostly:
  - Substitution
  - Permutation (or transposition)
  - XOR



Substitution

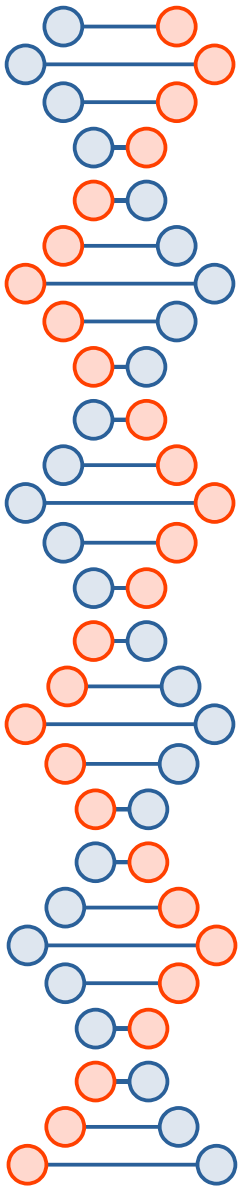
HELLO WORLD

TNWWX DXPWE



Permutation

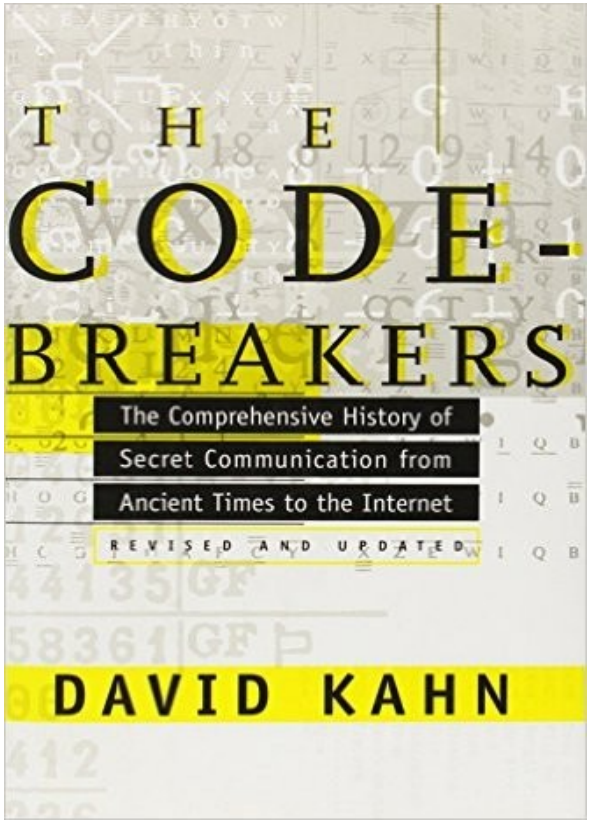
ABCD	ABDC	ACBD	ACDB	ADBC	ADCB
BACD	BADC	BCAD	BCDA	BDAC	BDCA
CABD	CADB	CBAD	CBDA	CDAB	CDBA
DABC	DACB	DBAC	DBCA	DCAB	DCBA

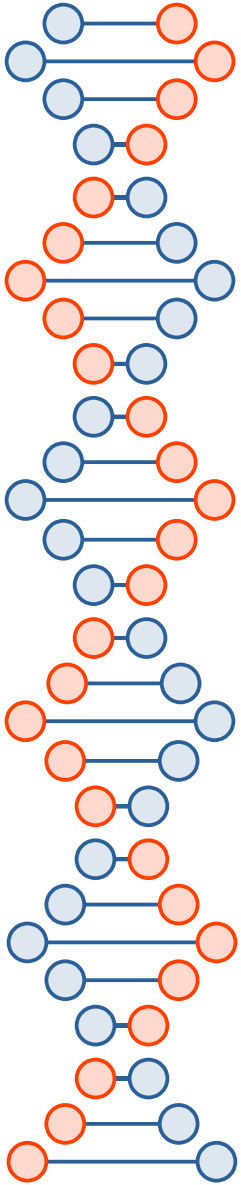


Bitwise XOR

$$
\begin{aligned}
&00101010_{\mathrm{b}} \\
\oplus\,&10000110_{\mathrm{b}} \\
=\,&10101100_{\mathrm{b}}
\end{aligned}
$$

2000+ years of history...



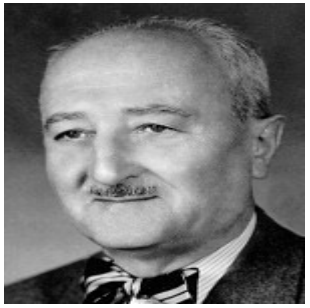


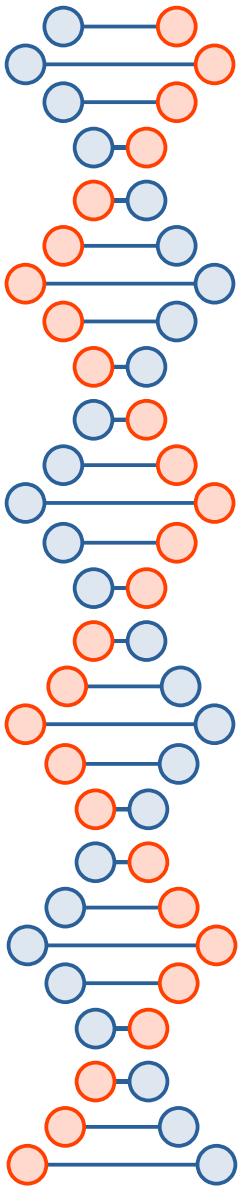
Symmetric encryption over time

- 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

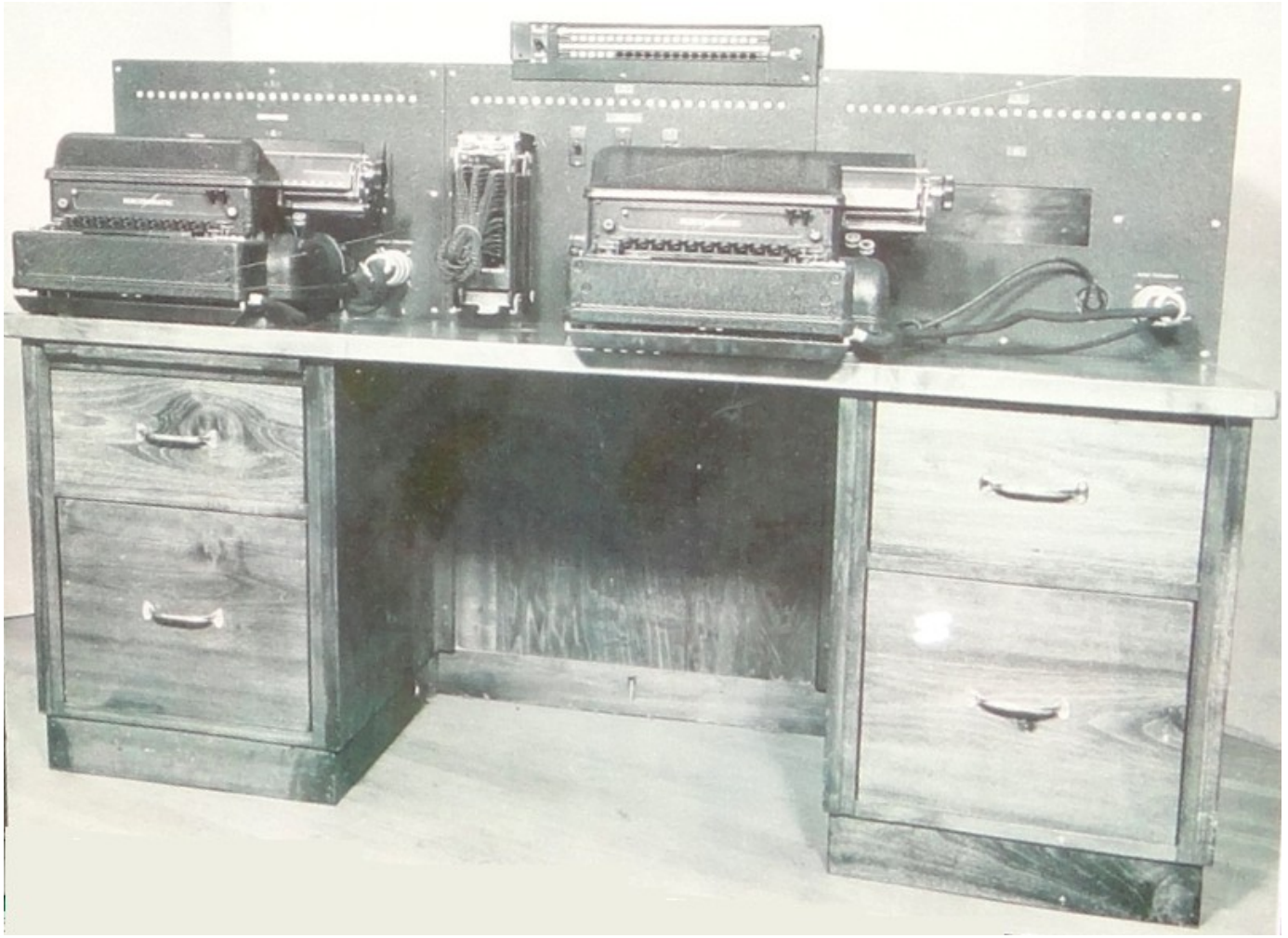
William and Elizabeth Friedman

- 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, conceived CryptoAG scheme





Substitution and/or permutation...

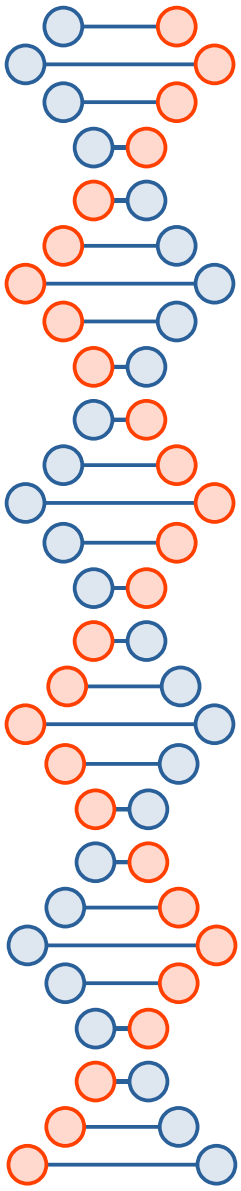


https://en.wikipedia.org/wiki/Type_B_Cipher_Machine#/media/File:Purple_cipher_machine_analog_bw_photo_NCM.jpg

https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

Zodiac cipher

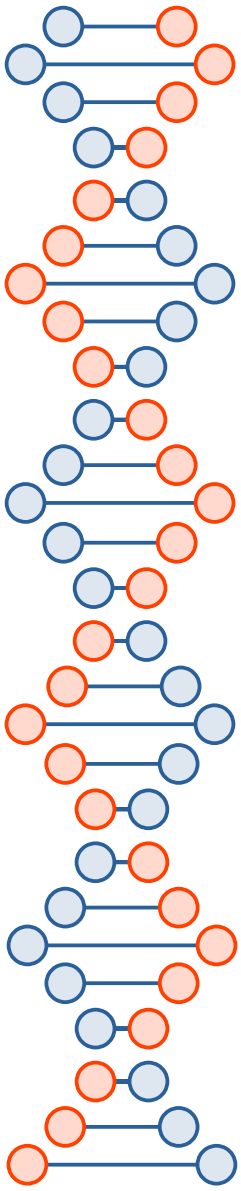
Image from wikia



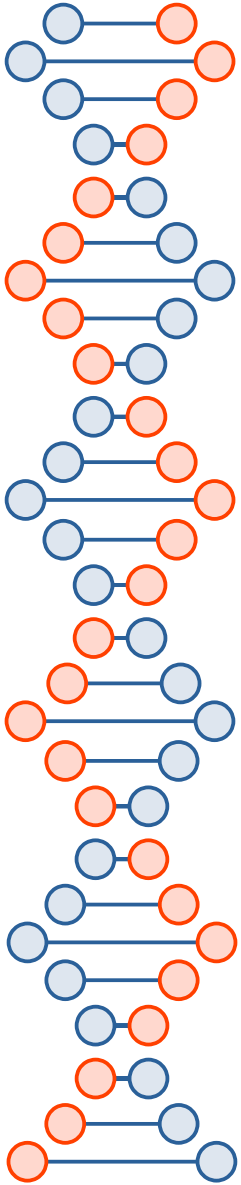
How to crack?

- Frequency analysis
- “The most common letter in the english language is e”
- “Gsv nlhg xlnnlm ovggvi rm gsv vmtorhs ozmtfztv rh v”
  - 7 v’s, 4 g’s, 4 m’s, 3 s’s, 3 n’s, 3 l’s …

- Guess what quantum computers are good at?

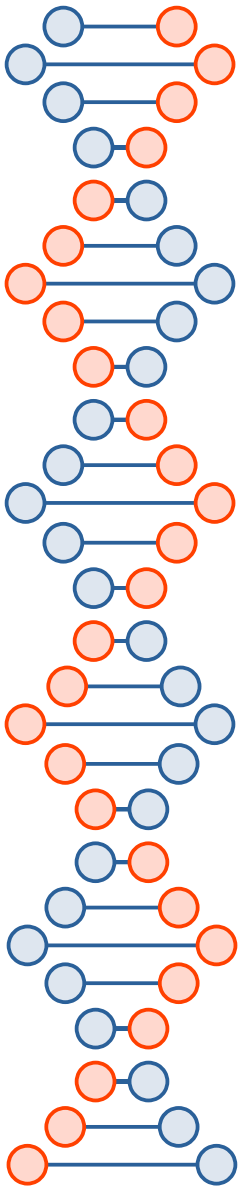


XOR...



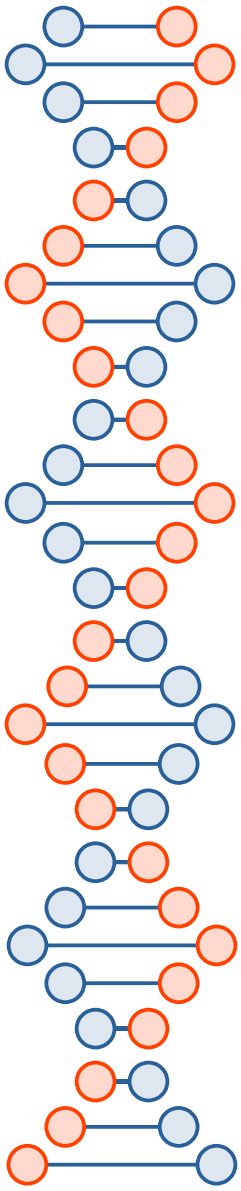
Bitwise XOR as a cipher itself

- 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

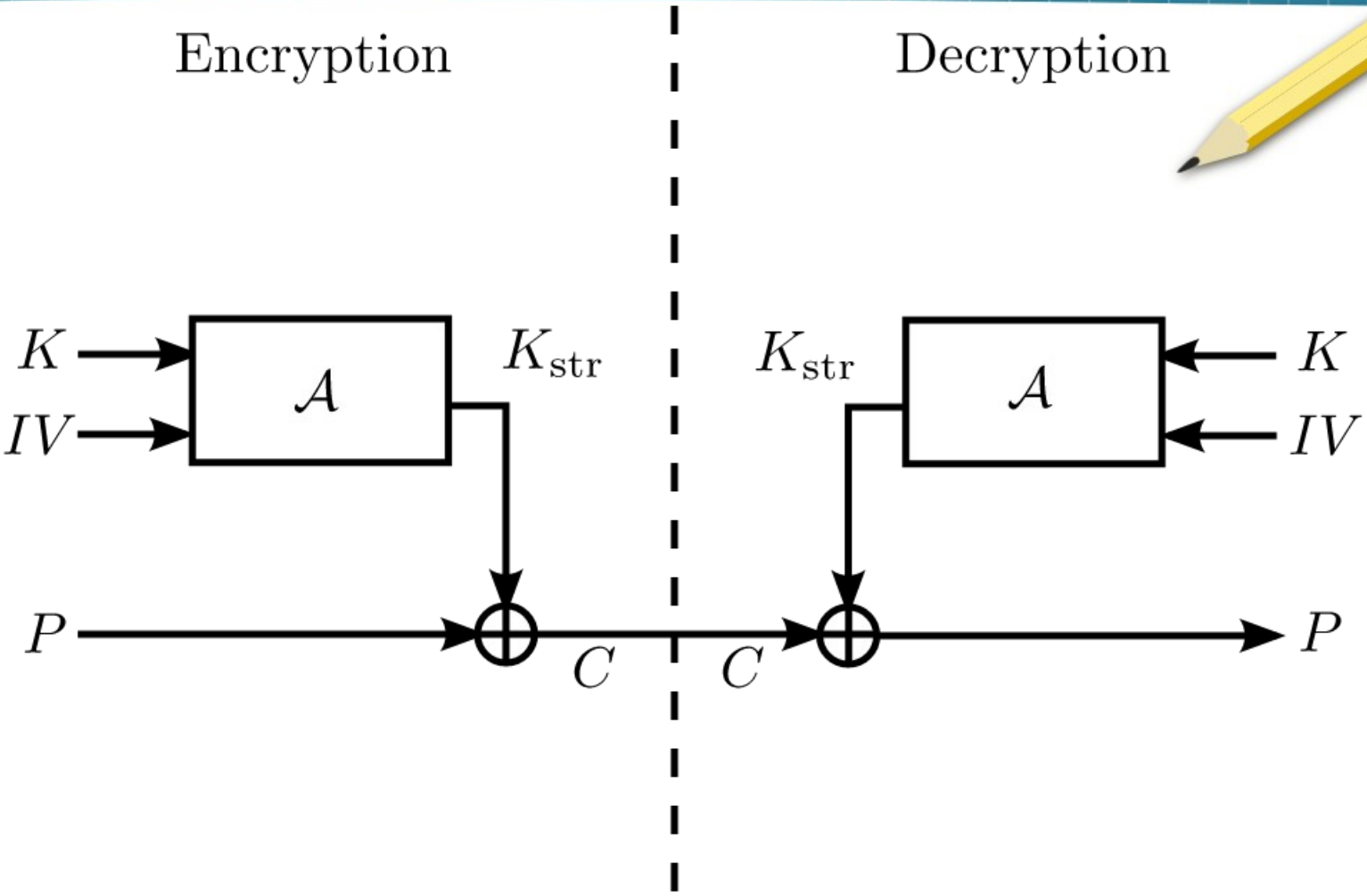


One-time pad

- *E.g.*, an XOR cipher or Caesar cipher where the key has good randomness and is as long as the plaintext
  - And never gets reused
  - Key is as long as the plaintext/ciphertext is
- Most codes made by the NSA through the 1980s were one-time pads
  - What if it's not practical to share enough key material beforehand, *e.g.*, on the Internet?

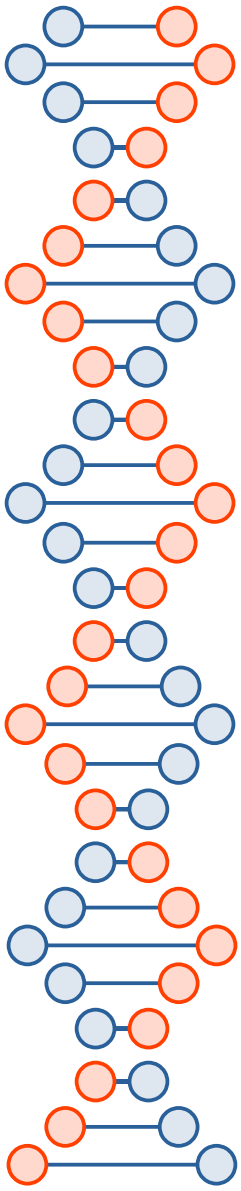


An attractive option that we'll talk about later is a stream cipher...



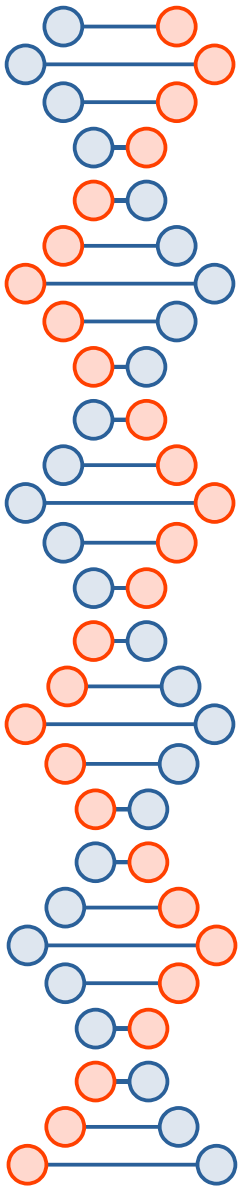
https://commons.wikimedia.org/wiki/File:Stream_cipher.svg

Because of the properties of XOR, it’s *dangerous* to reuse key material.



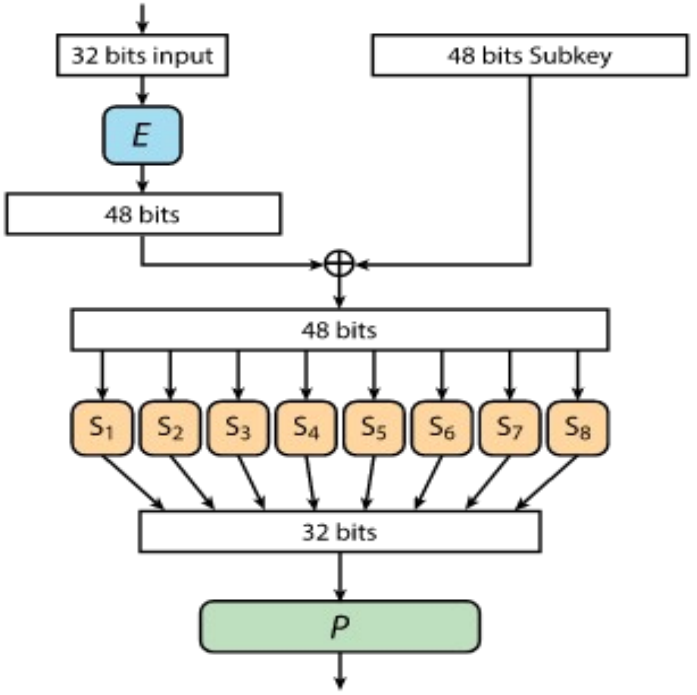
Preview:

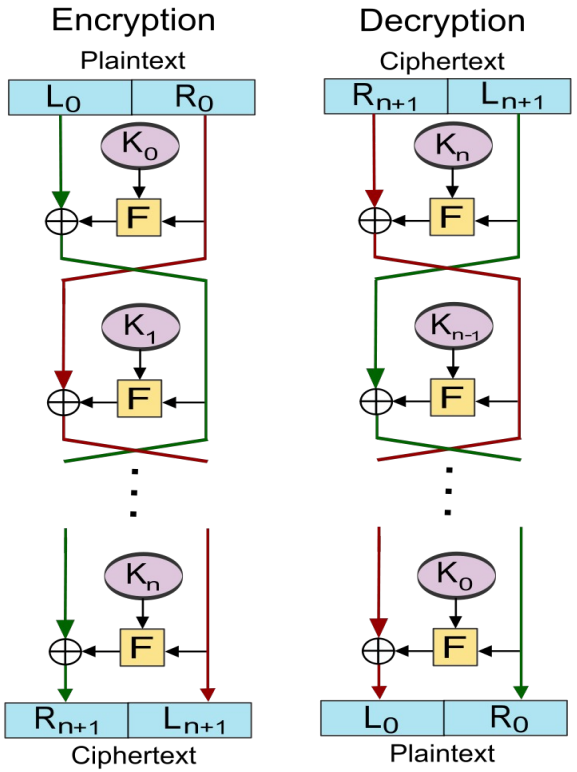
CNOT, the quantum version of XOR, will defy your concept of time and causality and we'll see that the outputs sometimes affect the inputs.

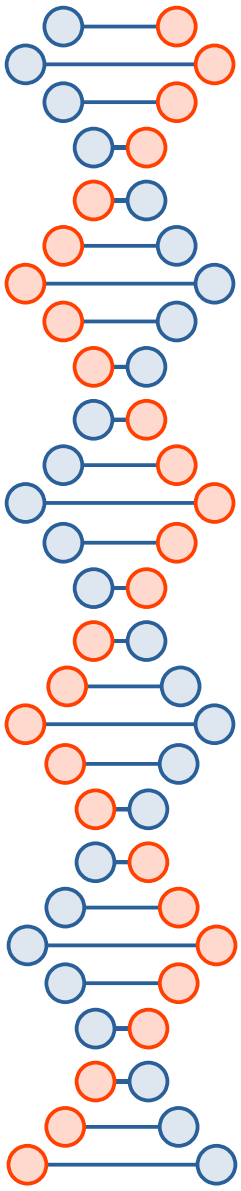


Now, let’s look at the first really good (in Jed’s opinion) symmetric cipher...

1977 - DES (16 rounds, 64-bit blocks, 56-bit key)



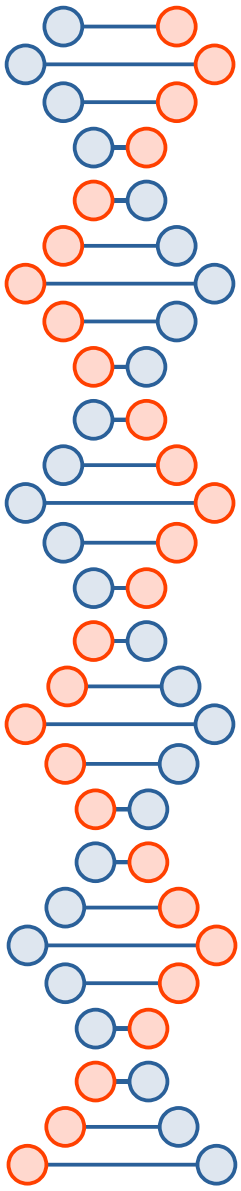




DES S-boxes

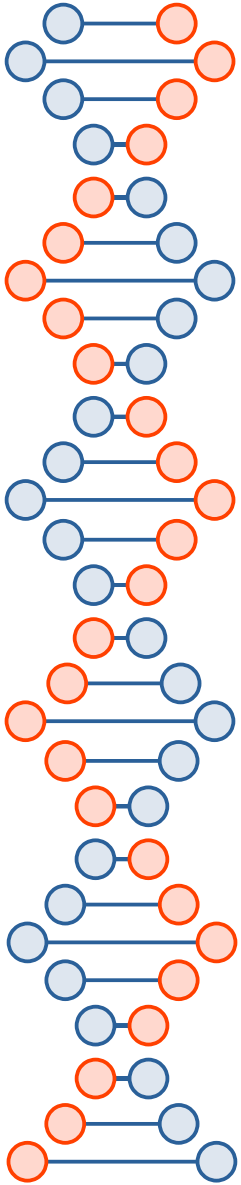
- 6 bits becomes 4 bits
- Values somewhat arbitrary
  - IBM proposed some, NSA replaced with others
    - Linear and differential cryptanalysis (unknown in the open literature at the time) were probably the reasons

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 (preview)

- 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)
- Blowfish used π as the S boxes
- *Preview:* AES is going to do something very clever, that is invertible (no need for the Feistel structure, so fewer rounds) but still thwarts linear and differential cryptanalysis.

What makes a good symmetric crypto algorithm?

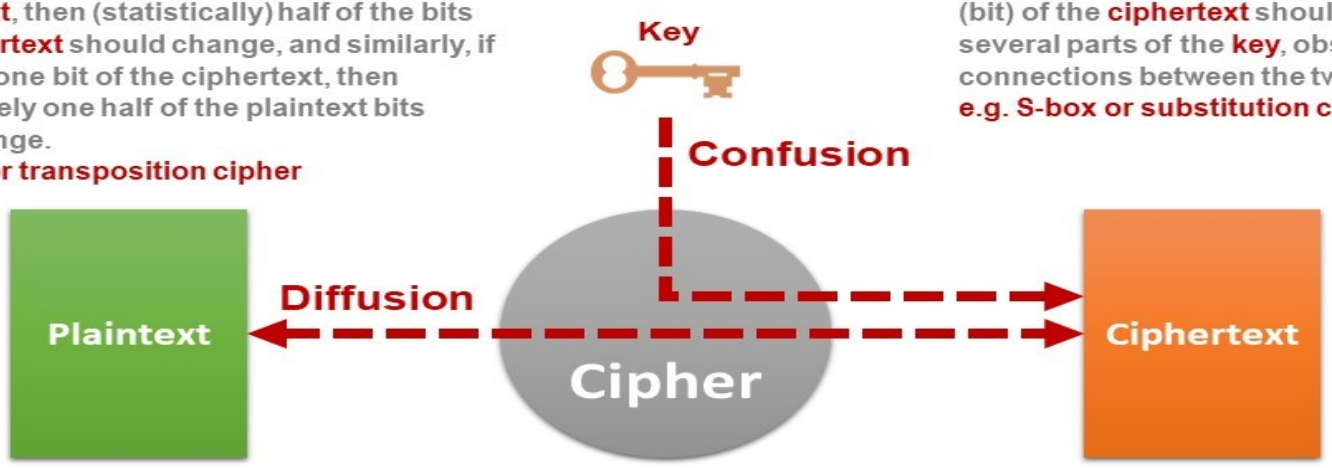
Lots of things, but two you should know are confusion and diffusion (diffusion is also known as the avalanche effect).

Claude Shannon, *A Mathematical Theory of Cryptography (1945 classified report)*

Confusion and Diffusion

Diffusion means that if we change a single bit of the **plaintext**, then (statistically) half of the bits in the **ciphertext** should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.
e.g. P-box or transposition cipher

Confusion means that each binary digit (bit) of the **ciphertext** should depend on several parts of the **key**, obscuring the connections between the two.
e.g. S-box or substitution cipher



https://en.wikipedia.org/wiki/Confusion_and_diffusion

https://wentzwu.com/2019/09/02/confusion-and-diffusion/

Attacks on block ciphers

- Linear and differential cryptanalysis
  - NSA must have known about these when giving input about DES, rest of the world found out in the 1990s
- Many others
  - E.g., rotational cryptanalysis
- CBC padding oracle attacks and others that are typically performed on live systems

For more details and the image source for the following two slides, see:
A Tutorial on Linear and Differential Cryptanalysis, by Howard M. Heys
https://jedcrandall.github.io/courses/cse539spring2023/ldc_tutorial.pdf

Linear cryptanalysis

- Solve for the key using plaintext/ciphertext pairs and linear approximations
- XOR is linear arithmetic modulo 2, permutations are also linear, only S-boxes save you

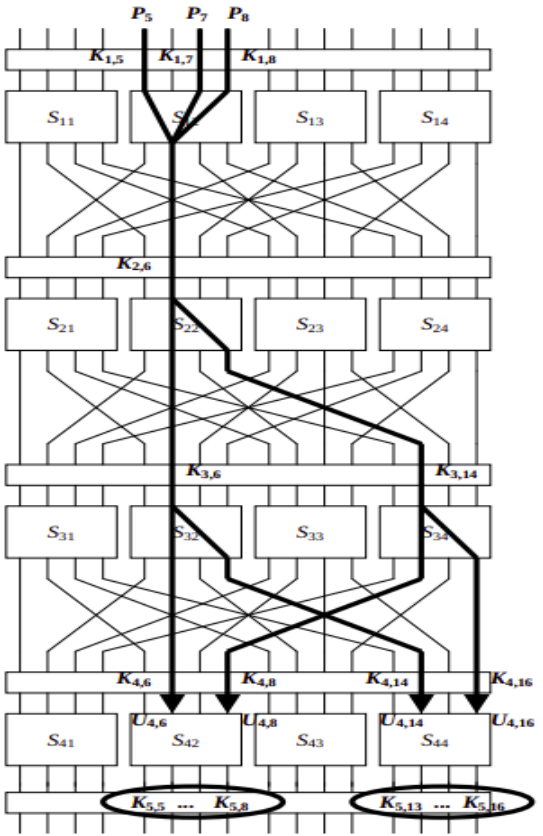


Figure 3. Sample Linear Approximation

Differential cryptanalysis

- Solve for key using plaintext/ciphertext pairs and propagated bit differences
- XOR and permutations don’t hide bit differences, only the S-boxes save you

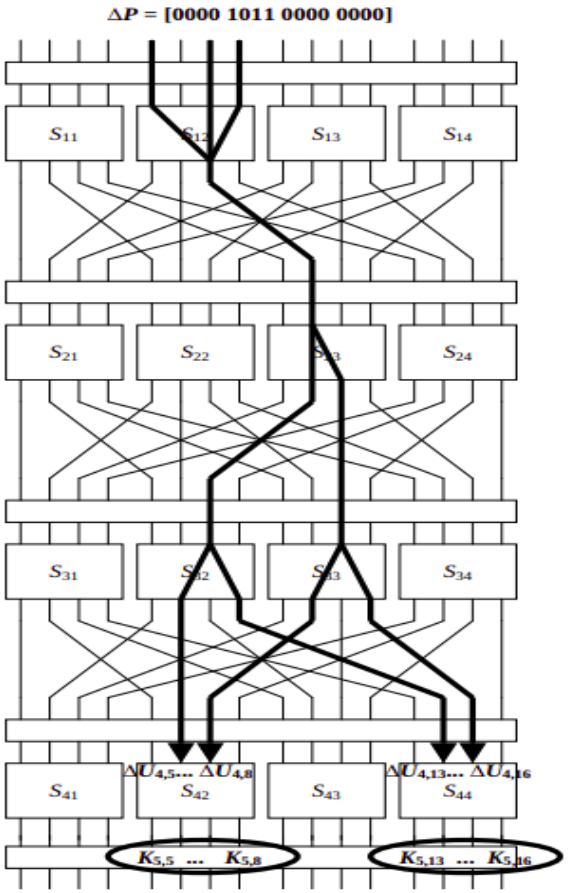
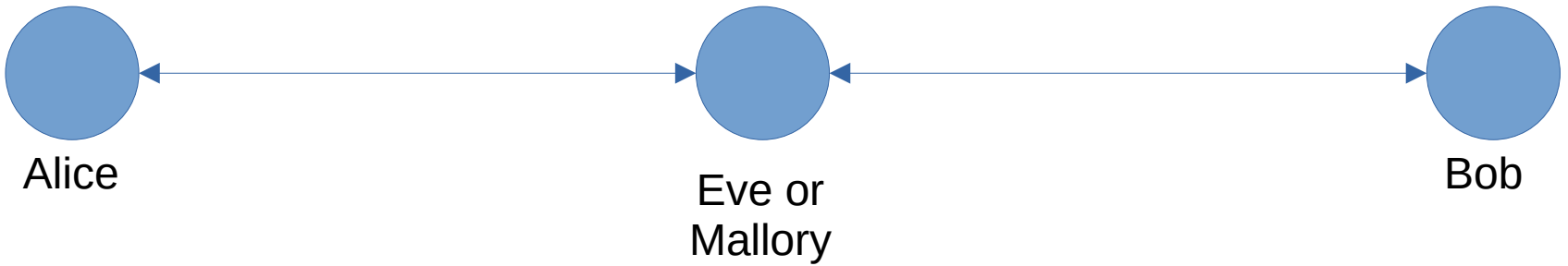
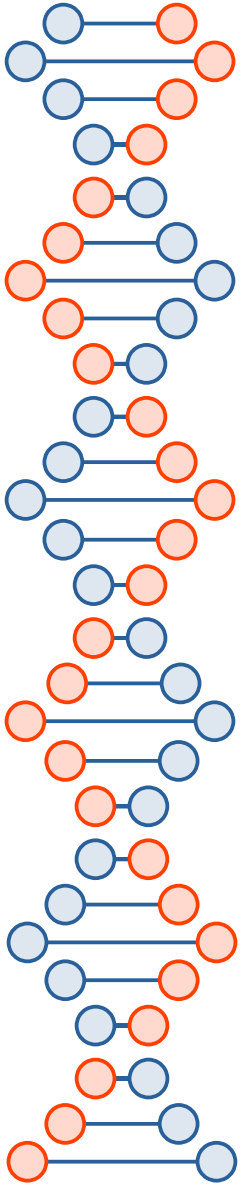


Figure 5. Sample Differential Characteristic

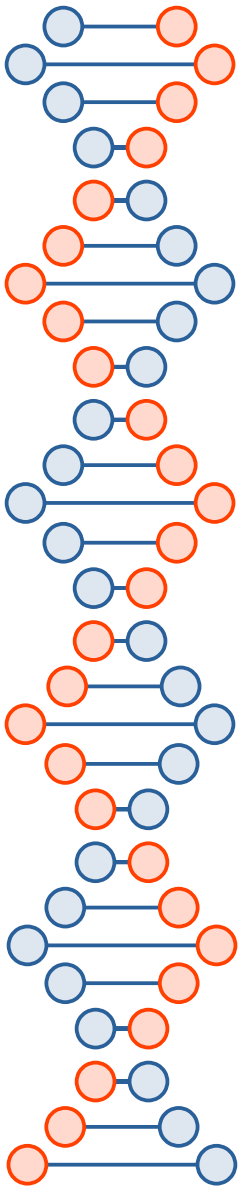


WiFi, electric path, or optical… Eve or Mallory get their own copy!
So how to Alice and Bob exchange a key?



A nice video about Diffie-Hellman

- https://www.youtube.com/watch?v=YEBfamv-_do



Darknet Diaries, Episode 83

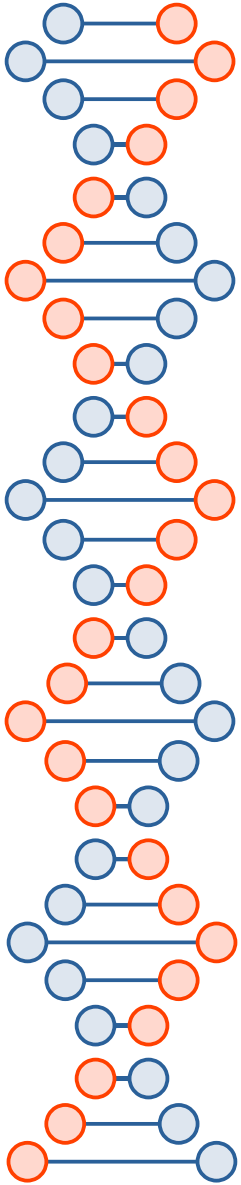
https://darknetdiaries.com/transcript/83/

- “There was no concept of doing anything cryptographic in terms of software back in the late 80s. I say this, I’m in contact with a fellow alumni from the InfoSec organization and people that were there years before I was, and I’ve asked. To the best that I have been able to figure out, what we ended up producing which was half paper pad, half key on a floppy, and a computer program that would do the encryption and decryption. That was the first foray into software-based cryptography that NSA produced.”

  --Jeff Man

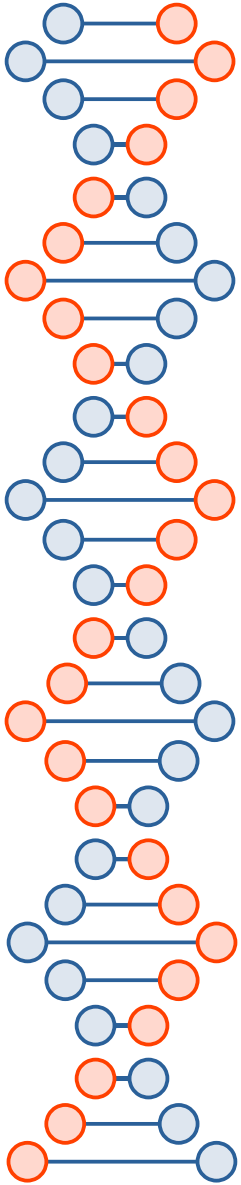

1 SYWAH TNMQG AIXSM MDBHQ TYRCO
2 OIBUA VBFAD HGSTR IQHJU CXHUW
3 ZIEZA UFOQY WMPKY SZWHJ LIYAŚ
4 JNHHY KCQKR ORPKJ PMYBU ZUKNA
5 JIHMW RVAUP XSHXR SGGSV
6 OPTQG PVCBT PMWLY MCEU
KBVT RXP
IRCXH
NXSDP
ACUPC
PIYJG
TARFP
Crypto Museum
cryptomuseum.com


PX 1000Cr
Druk op ON/STOP om het apparaat aan te zetten of uit.
CLEAR ALL
CLR LINE
CODE
KEY
Zie achterzijde voor het verzenden van tekst.
LIST
PRINT
RCVE
LOW HIGH MARGIN
SET CLR TAB
CAPS LOCK
SHIFT
INS TXT
INSERT
DEL TXT
DELETE
SEARCH
TEXT
LOAD
DUMP
KEY TXT
CODE
CLR LINE
CLEAR ALL
ON
STOP



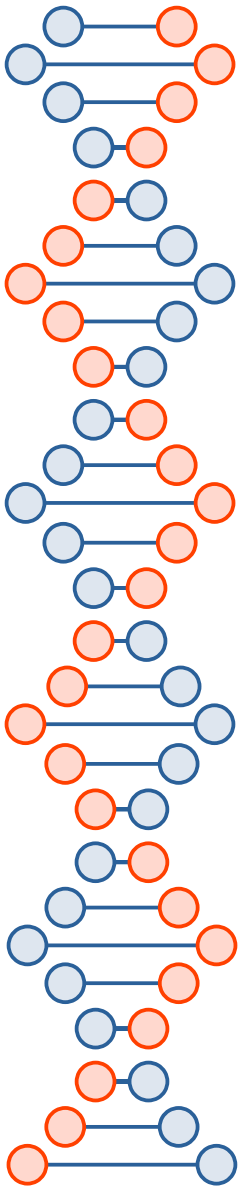
Couple of footnotes

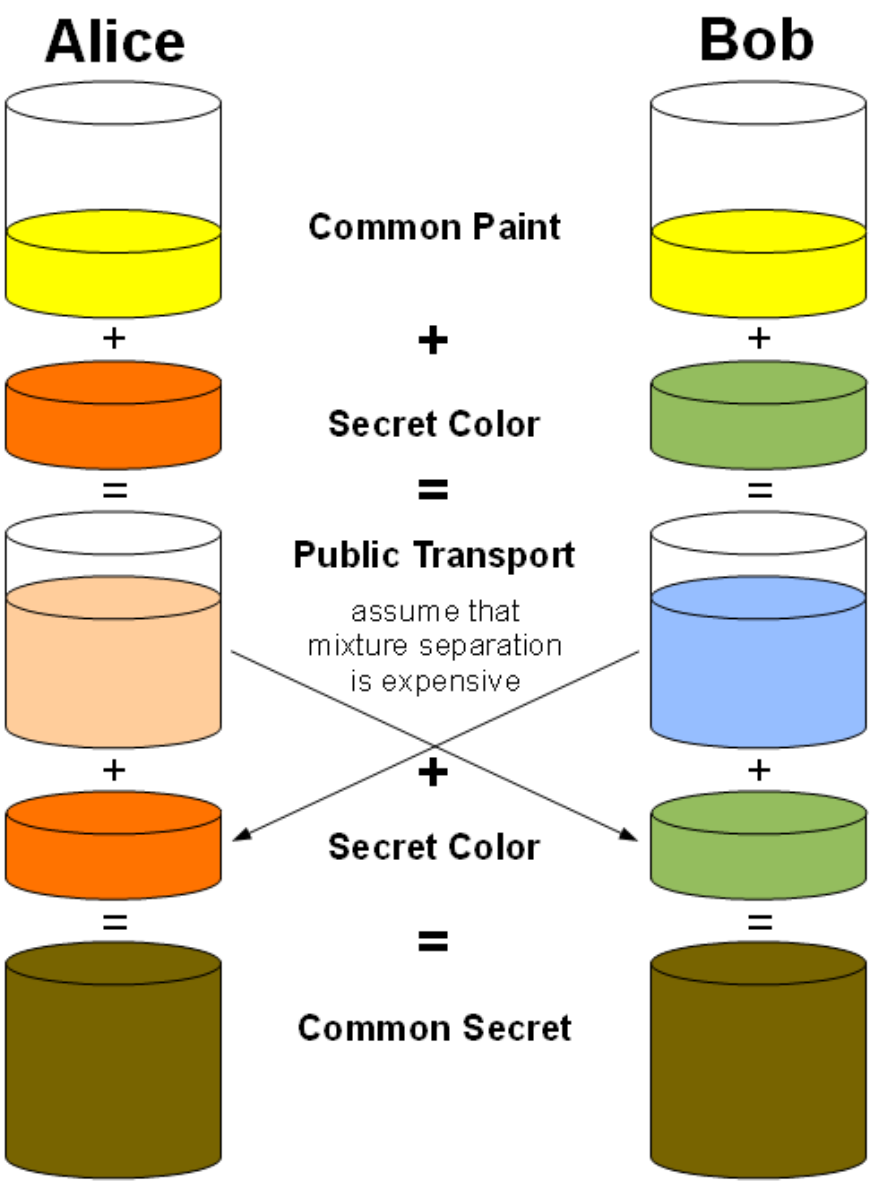
- Diffie-Hellman-Merkle?
- Who was first?
  - Diffie-Hellman conceived and then published 1976
  - GCHQ version conceived 1969, published 1997



Basics...

- https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange




Alice
Bob
Common Paint
+
Secret Color
=
Public Transport
assume that
mixture separation
is expensive
+
Secret Color
=
Common Secret

Alice		Bob		Eve	
Known	Unknown	Known	Unknown	Known	Unknown
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\mathbf{a = 6}$	$\mathbf{b}$	$\mathbf{b = 15}$	$\mathbf{a}$		$\mathbf{a}$, $\mathbf{b}$
$A = 5^{a} \bmod 23$		$B = 5^{b} \bmod 23$			
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\mathbf{B = 19}$		$\mathbf{A = 8}$		$A = 8, B = 19$	
$\mathbf{s} = B^{a} \bmod 23$		$\mathbf{s} = A^{b} \bmod 23$			
$\mathbf{s} = 19^{6} \bmod 23 = \mathbf{2}$		$\mathbf{s} = 8^{15} \bmod 23 = \mathbf{2}$			$\mathbf{s}$

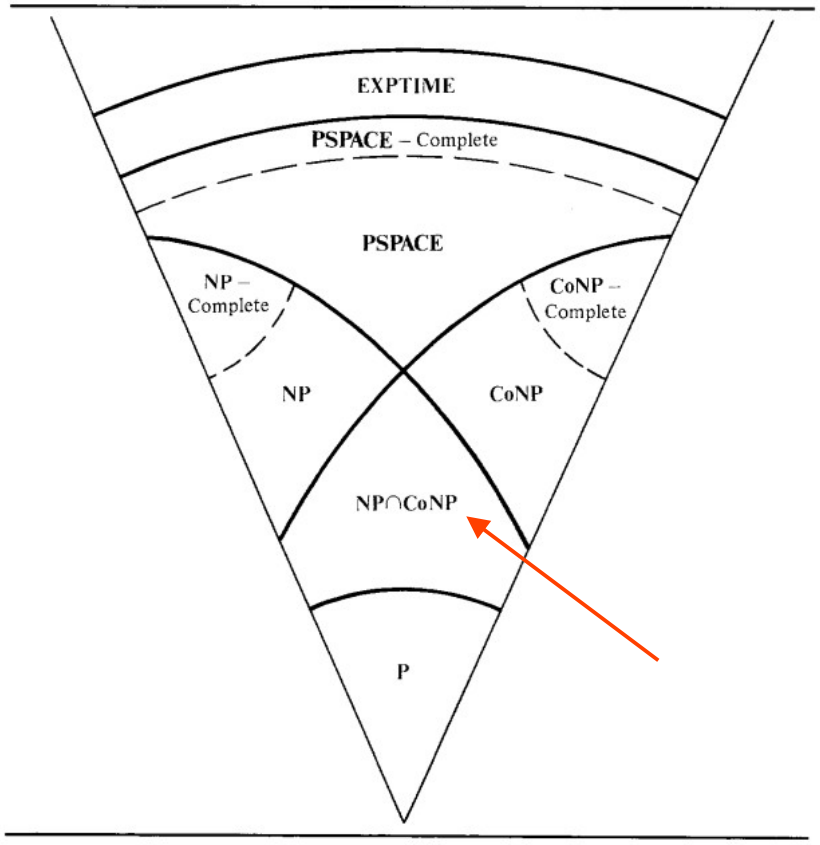
The paper...

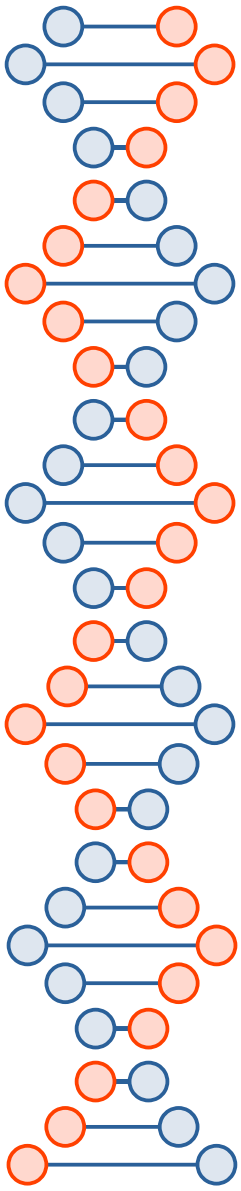
I. Introduction

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

https://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

FIGURE 1.18 Complexity classes.





In order to develop large, secure, telecommunications systems, this must be changed. A large number of users n results in an even larger number, $(n^2 - n)/2$ potential pairs who may wish to communicate privately from all others.

The new technique makes use of the apparent difficulty of computing logarithms over a finite field $GF(q)$ with a prime number q of elements. Let

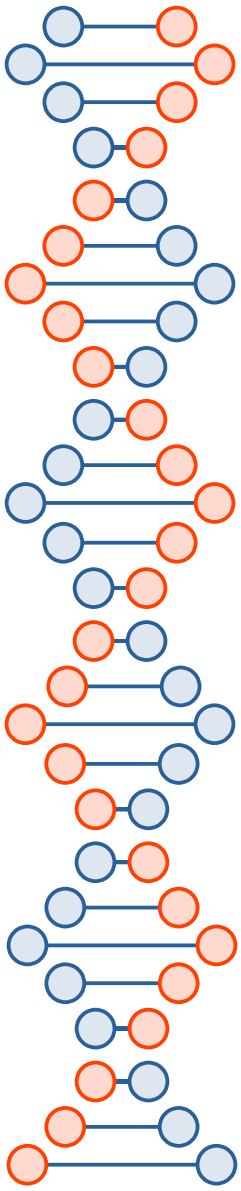
$$Y = \alpha^X \bmod q, \qquad \text{for } 1 \leq X \leq q - 1, \tag{4}$$

where α is a fixed primitive element of $GF(q)$, then X is referred to as the logarithm of Y to the base α, mod q:

$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \leq Y \leq q - 1. \tag{5}$$

Calculation of Y from X is easy, taking at most $2 \times \log_2 q$ multiplications [6, pp. 398–422]. For example, for $X = 18$,

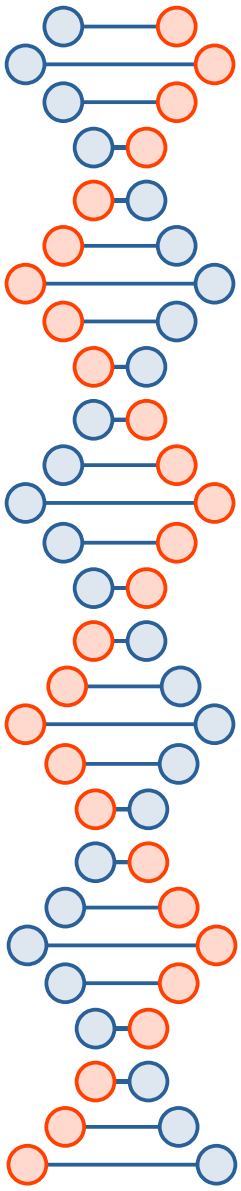
$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2. \tag{6}$$



tation time must be small. A million instructions (costing approximately $0.10 at bicentennial prices) seems to be a reasonable limit on this computation. If we could ensure,

There is currently little evidence for the existence of trap-door ciphers. However they are a distinct possibility and should be remembered when accepting a cryptosystem from a possible opponent [12].

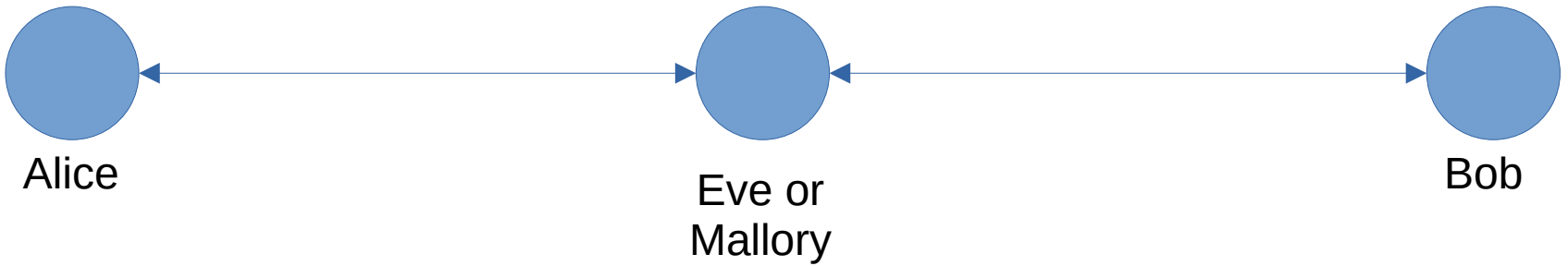
Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.



We assume that the function f is public information, so that it is not ignorance of f which makes calculation of f^{-1} difficult. Such functions are called one-way functions and were first employed for use in login procedures by R. M. Needham [9, p. 91]. They are also discussed in two recent papers [10], [11] which suggest interesting approaches to the design of one-way functions.

More precisely, a function f is a *one-way function* if, for any argument x in the domain of f, it is easy to compute the corresponding value $f(x)$, yet, for almost all y in the range of f, it is computationally infeasible to solve the equation $y = f(x)$ for any suitable argument x.

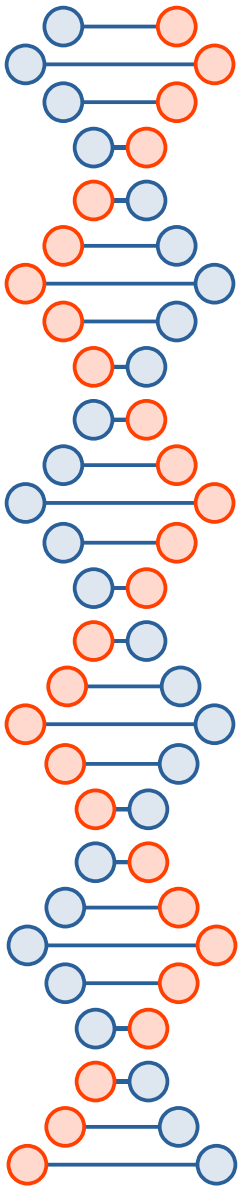
pp. 415, 420, 422–424]. We hope this will inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly.



WiFi, electric path, or optical… Eve or Mallory get their own copy!

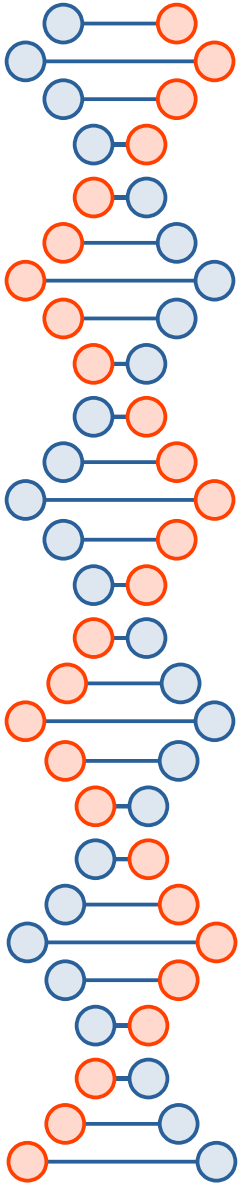
Mallory gets to change things!

How does Alice know she's talking to Bob (or *vice versa*)?



Asymmetric crypto

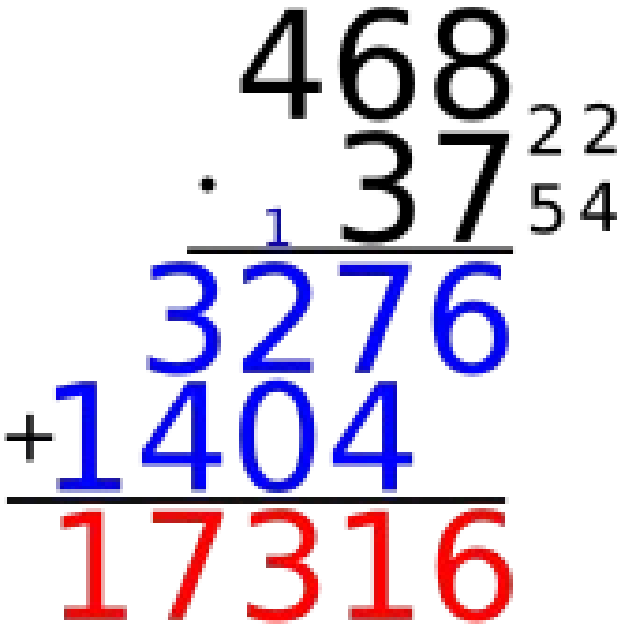
- Some people use “public key crypto” to generally refer to all of asymmetric crypto
- Goes beyond Diffie-Hellman and RSA
  - *E.g.*, elliptic curve crypto
  - Quantum resistant
- Goes well beyond encryption, authentication, non-repudiation (signatures), and key exchange
  - Oblivious transfer, secure multiparty computation, cryptocurrencies, identity-based encryption, secret sharing, zero-knowledge proof, private information retrieval, cryptocounters, subliminal channels, ransomware, deniable encryption, off-the-record, forward secrecy, future secrecy, ...



RSA *vs.* DH

- Diffie-Hellman (1976)
  - Key exchange
  - *Both sides get to choose something random*
- RSA (1977)
  - Encryption
  - Signatures

Multiplication is polynomial time in number of digits ($O(n^2)$ or $O(n \log n)$)



Modular exponentiation

$153^{189} \pmod{251}$

Naive way: multiply 153 times itself 189 times. Won't work for, *e.g.*, 2048-bit numbers in the exponent

Better way (all mod 251)

$153^0 = 1$

$153^1 = 153$

$153^2 = 66$

$153^4 = 89$

$153^8 = 140$

$153^{16} = 22$

$153^{32} = 233$

$153^{64} = 73$

$153^{128} = 58$

1. Repeated squaring

2. Don’t forget the modulus

Better way

- 189 in binary is 0b10111101
- $189 = 1*2^7 + 0*2^6 + 1*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0$
- $153^{189} \pmod{251} = 153^{(128+0+32+16+8+4+0+1)} \pmod{251}$

  $= 153^{128} * 153^{32} * 153^{16} * 153^{8} * 153^{4} * 153^{1} \pmod{251}$

  $= 58 * 233 * 22 * 140 * 89 * 153 \pmod{251}$

  $= 73$

WolframAlpha computational intelligence

58 * 233 * 22 * 140 * 89 * 153 (mod 251)

NATURAL LANGUAGE | MATH INPUT | EXTENDED KEYBOARD | EXAMPLES | UPLOAD | RANDOM

Input

$(58 \times 233 \times 22 \times 140 \times 89 \times 153) \bmod 251$

Result

73

WolframAlpha computational intelligence

(153^189) mod 251

NATURAL LANGUAGE | MATH INPUT | EXTENDED KEYBOARD | EXAMPLES | UPLOAD | RANDOM

Input

$153^{189} \bmod 251$

Result

73

$$153^{189} = 73 \pmod{251}$$
$$189 = \log_{153} 73 \pmod{251}$$

$$153^{???} = 73 \pmod{251}$$
$$??? = \log_{153} 73 \pmod{251}$$

This is called the discrete logarithm, and there is no known algorithm for solving it in the general case that is polynomial in the number of digits.

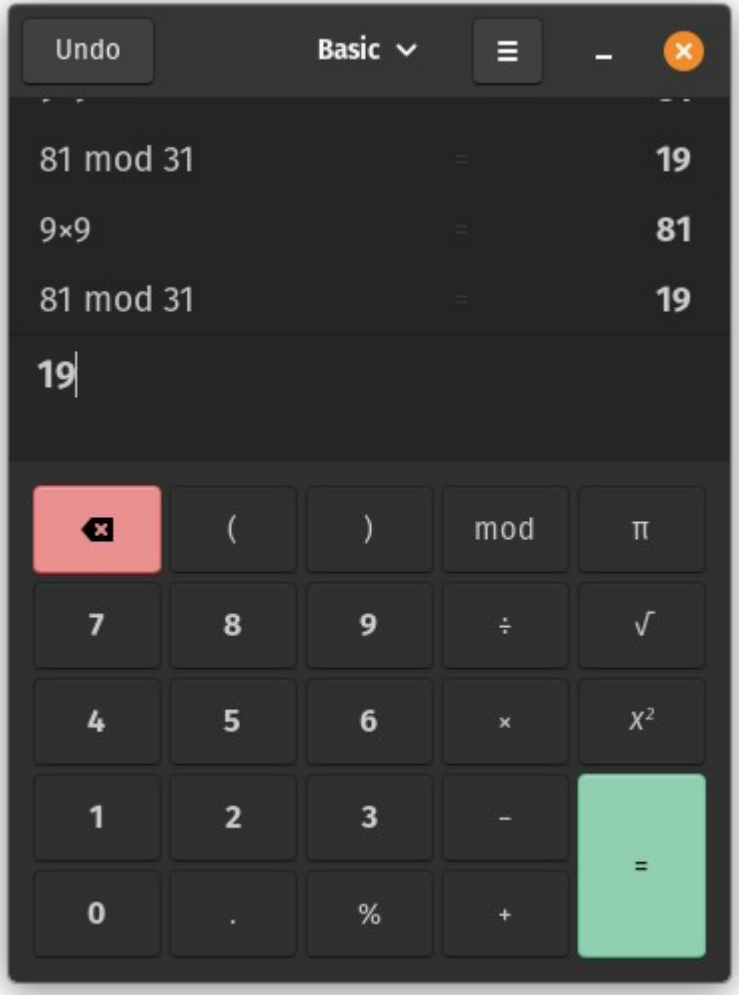
$$153^{189} = 73 \pmod{251}$$
$$153^{64} = 73 \pmod{251}$$

$$153^{189} \equiv 73 \pmod{251}$$
$$153^{64} \equiv 73 \pmod{251}$$

$$153^{189} \equiv 153^{64} \equiv 73 \pmod{251}$$

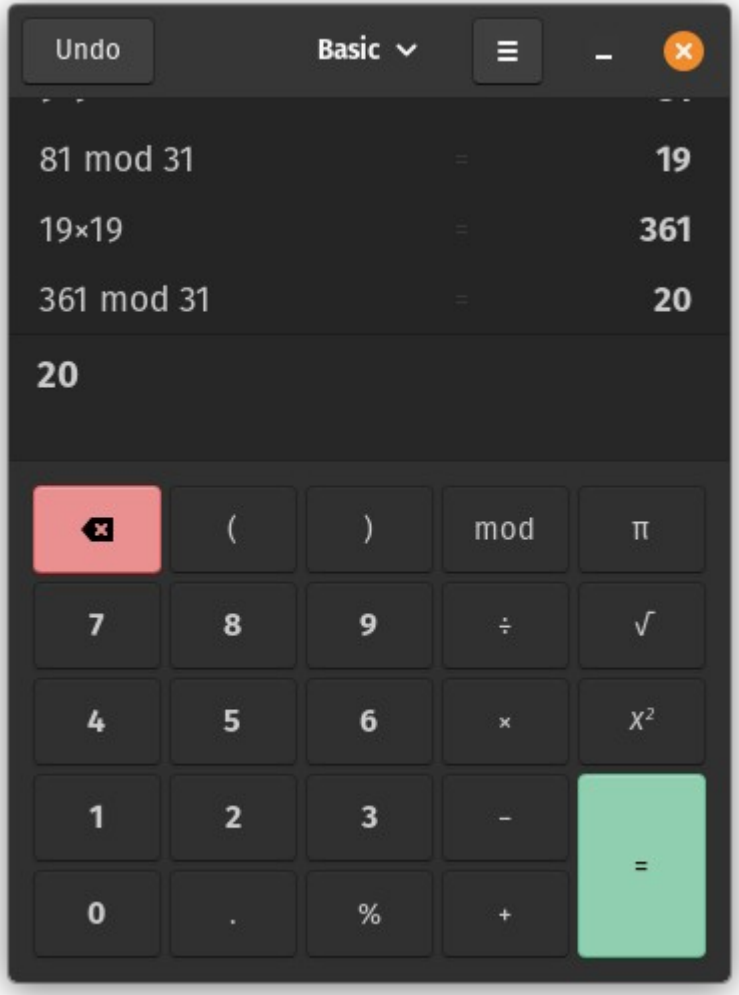
An example…

- 3^{17} mod 31
- 17 = 16 + 1
- $16 = 2^4$, $(((3^2)^2)^2)^2 = 3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, …


Undo
Basic
81 mod 31 = 19
9×9 = 81
81 mod 31 = 19
19
( ) mod π
7 8 9 ÷ √
4 5 6 × X²
1 2 3 −
0 . % +
=

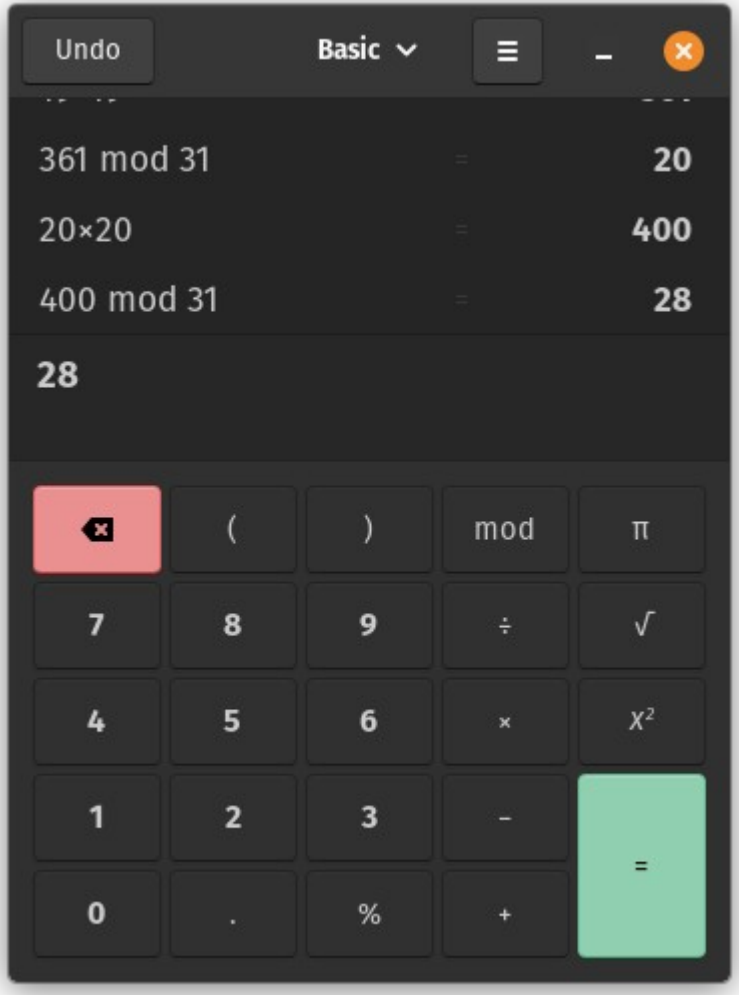
An example…

- 3^{17} mod 31
- 17 = 16 + 1
- 16 = 2^4 , $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, …


Undo
Basic
81 mod 31 = 19
19×19 = 361
361 mod 31 = 20
20
( ) mod π
7 8 9 ÷ √
4 5 6 × X²
1 2 3 −
0 . % +
=

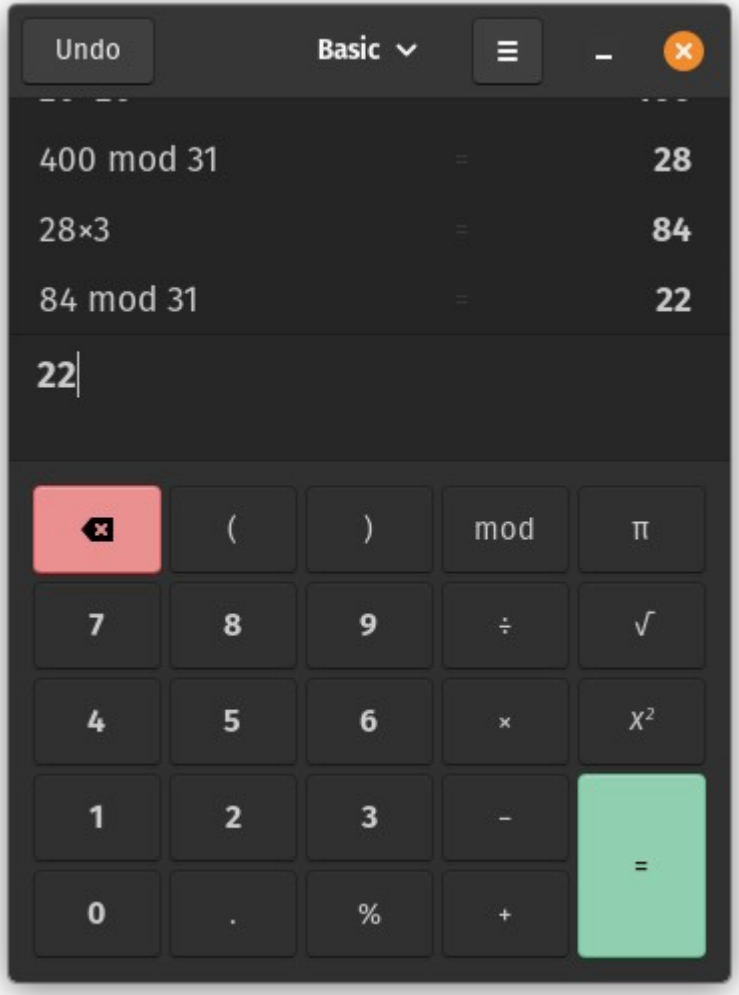
An example…

- 3^{17} mod 31
- 17 = 16 + 1
- 16 = 2^4 , $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, …


Undo
Basic
361 mod 31 = 20
20×20 = 400
400 mod 31 = 28
28
( ) mod π
7 8 9 ÷ √
4 5 6 × X²
1 2 3 −
0 . % +
=

An example…

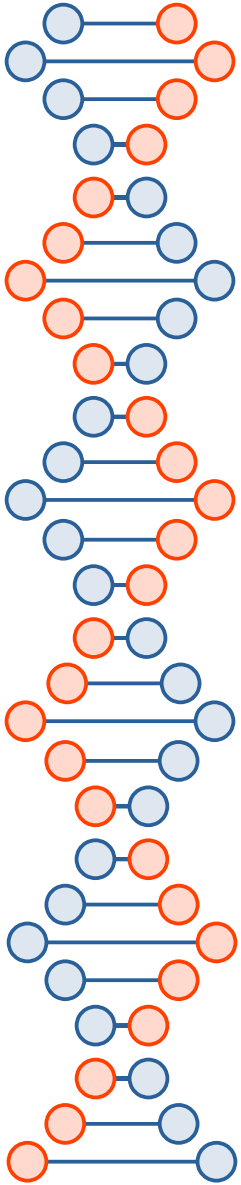
- 3^{17} mod 31
- 17 = 16 + 1
- 16 = 2^4 , $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, $3^{16}=28$…


Undo
Basic
400 mod 31 = 28
28×3 = 84
84 mod 31 = 22
22
( ) mod π
7 8 9 ÷ √
4 5 6 × X²
1 2 3 −
0 . % +
=

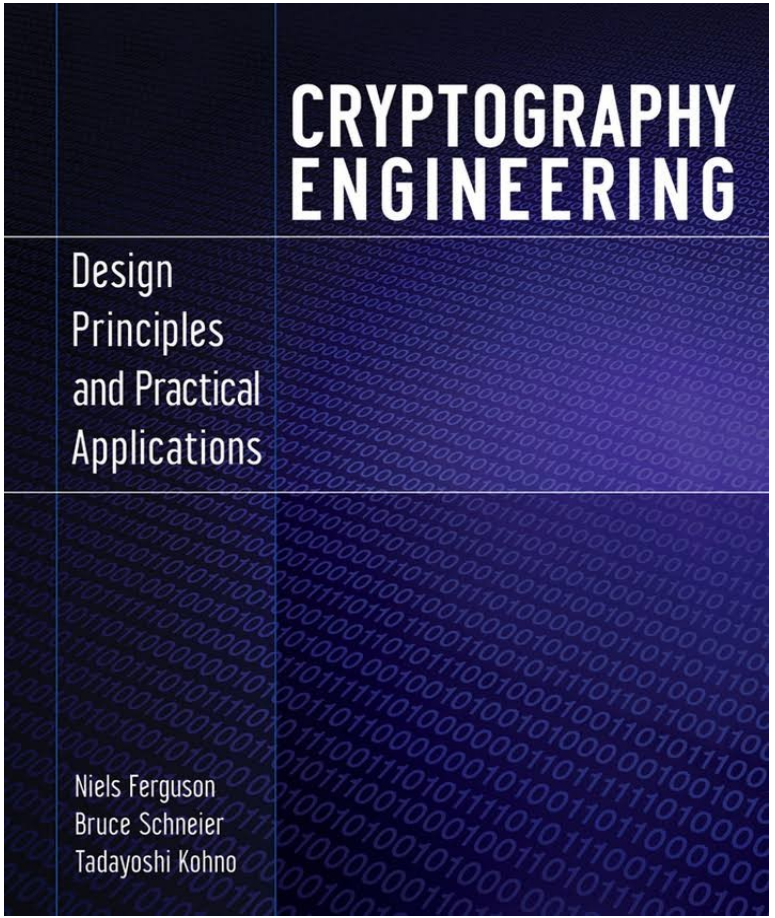
An example…

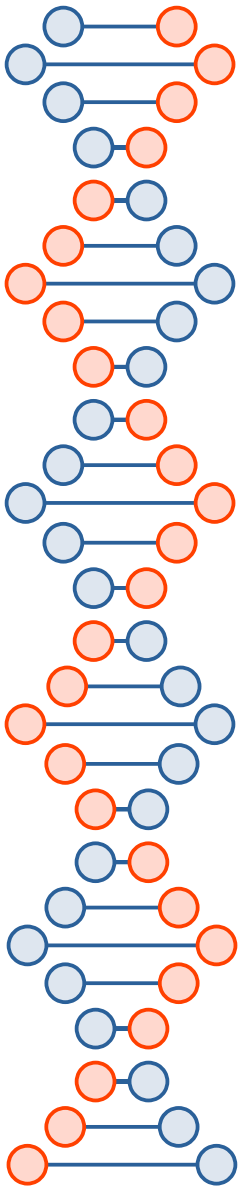
- $3^{17} \bmod 31 = 3^{16}3^{1} \bmod 31 = 22$
- $17 = 16 + 1$
- $16 = 2^4$, $(((3^2)^2)^2)^2=3^{16}$
- All mod 31…
  - $3^1=3$, $3^2=9$, $3^4=19$, $3^8=20$, $3^{16}=28$…

17 in binary is 0b10001



Cryptography Engineering by Ferguson *et al.*





Acknowledgments and resources

- Many of the above images are from Wikipedia
- https://www.youtube.com/watch?v=5mB_FUyfuZE&list=PLmh4YIWteoGgh0E2EuS4ZpzIi7ZhIW9Xp