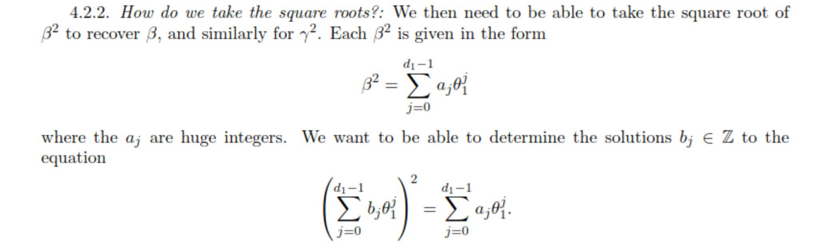
Math Club 1/26

Sign in on paper :)

Cryptography

What is Cryptography?

- Cryptography is the study of techniques for secure communications
    - Any communication that has to be secured (login info, government secrets, etc) uses cryptography
- Cryptography (especially modern!) is basically just another mask for applied math



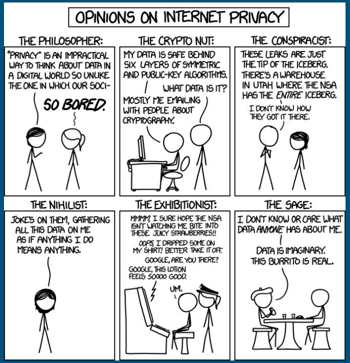
4.2.2. *How do we take the square roots?:* We then need to be able to take the square root of β^2 to recover β, and similarly for γ^2. Each β^2 is given in the form

$$\beta^2 = \sum_{j=0}^{d_1-1} a_j \theta_1^j$$

where the a_j are huge integers. We want to be able to determine the solutions $b_j \in \mathbb{Z}$ to the equation

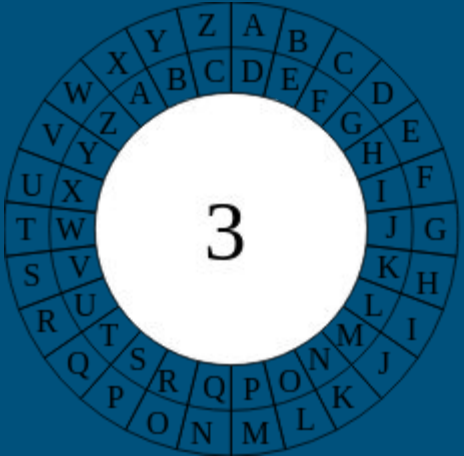
$$\left(\sum_{j=0}^{d_1-1} b_j \theta_1^j \right)^2 = \sum_{j=0}^{d_1-1} a_j \theta_1^j.$$

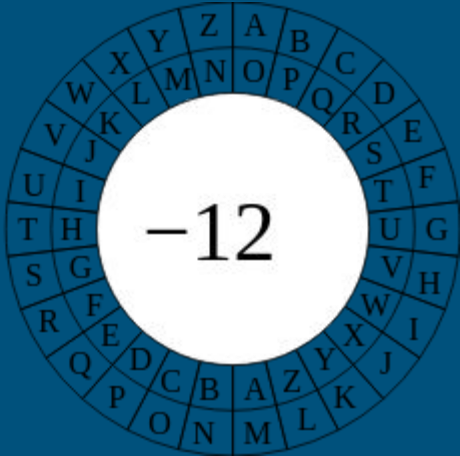
Figure 1: Random page on Cryptography textbook


OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

Historical ciphers

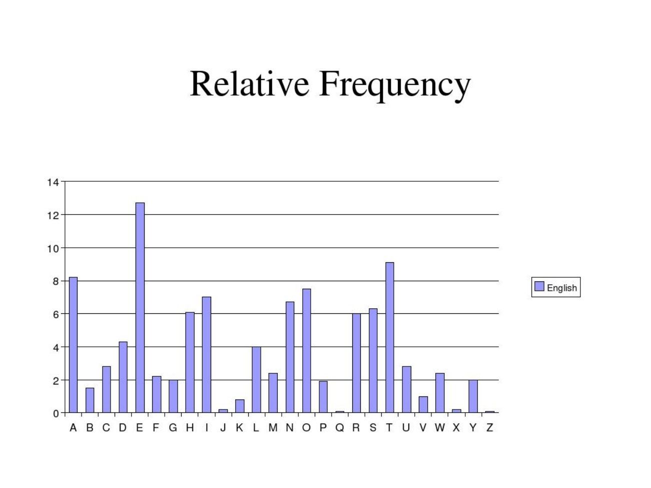
- Ciphers have been in use for thousands of years!
- Perhaps one of the most famous examples is the Caesar cipher
  - Slave's heads were tattooed and concealed under regrown hair
  - Invisible ink

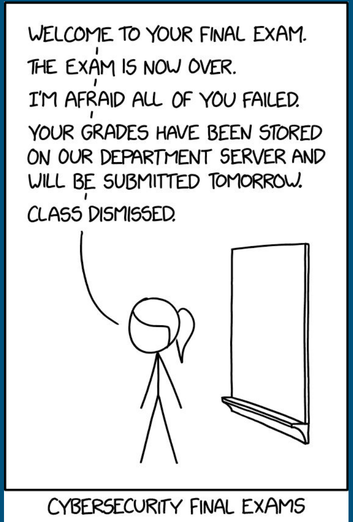

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
3


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
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
−12

Cracking methods

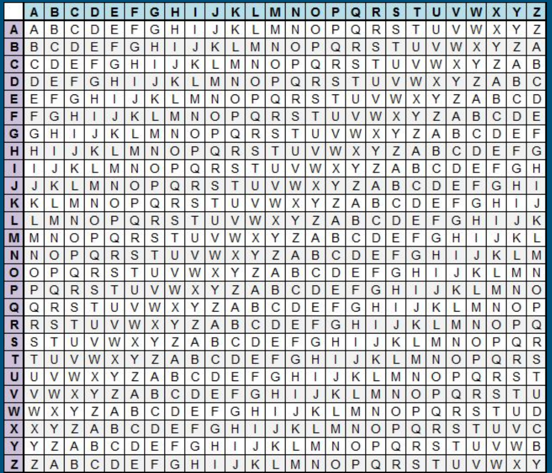
- **Frequency Analysis** - against a monoalphabetic cipher, looking at the frequency different letters appear is a very powerful strategy
- **Brute Force** - a surprisingly effective strategy. A lot of current attacks involve just reducing the complexity and letting brute force do the rest. DES fell to brute force and Moore's law
- **Differential Cryptanalysis** - find where non-random behavior is being exhibited and exploit that property



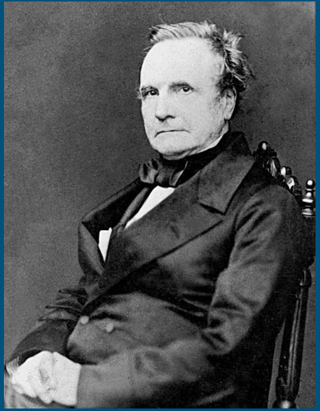

WELCOME TO YOUR FINAL EXAM.
THE EXAM IS NOW OVER.
I'M AFRAID ALL OF YOU FAILED.
YOUR GRADES HAVE BEEN STORED ON OUR DEPARTMENT SERVER AND WILL BE SUBMITTED TOMORROW.
CLASS DISMISSED.
CYBERSECURITY FINAL EXAMS

The Vigenere Cipher

- The Vigenere Cipher, first described in 1553 by Giovan Bellaso, was uncracked for 3 decades
- However, it fell victim to differential cryptanalysis by Charles Babbage in the 19th century



	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	D
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	C
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	B
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



Shannon’s Maxim

- "The enemy knows the system." - Claude Shannon
- One of the main principles in cryptography is that the adversary should be able to know everything but the key and still not be able to crack the system
- Anything that relies on a secretive system is bound to fail in the modern day given the amount of computing power available

Modern ciphers

- With the advent of computers, brute force has become a real problem
- DES (Data Encryption Standard) required 2^56 time to break
    - While this was not in the least feasible when it was formulated, Moore’s law quickly made it so that it could be cracked pretty easily using nothing but brute force in a few days by the end of the 20th century
- Modern cryptography has to deal with these problems, along with a myriad of other problems that come from advances in mathematics (ie meet in the middle and integral attacks)
- Currently ciphers can be classified into two groups: Symmetric-key and Asymmetric-key

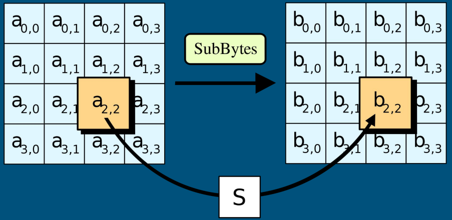
Symmetric Key

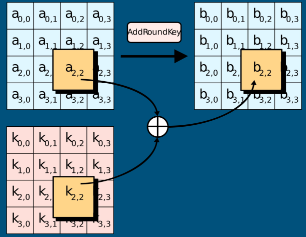
- Symmetric Key cryptography relies on a secret key shared between the sender and receiver
- Examples include the AES cipher
- Typically a block cipher or stream cipher
    - Block ciphers process data in fixed blocks
    - Stream ciphers encrypt one bit at a time
- One main weakness is that both people will have to have the secret key

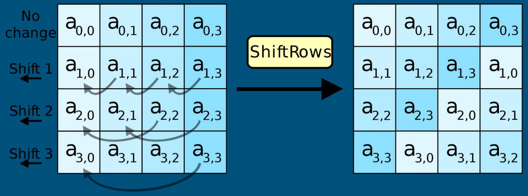
THE APP WILL LET YOU SEND MESSAGES TO YOUR FRIEND ROBERT, OR MY BROTHER.
CAN THEY REPLY?
NO.
MY NEW SECURE TEXTING APP ONLY ALLOWS PEOPLE NAMED ALICE TO SEND MESSAGES TO PEOPLE NAMED BOB.

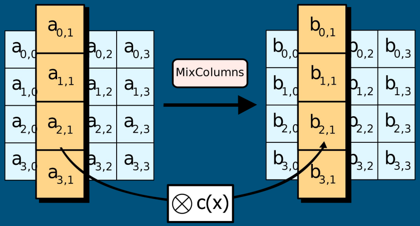
Rijndael (AES) cipher

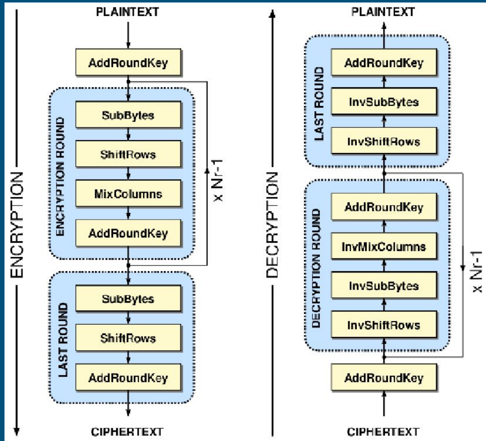
- Current US Standard for encryption





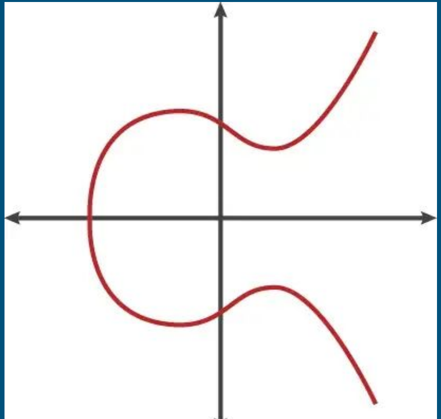


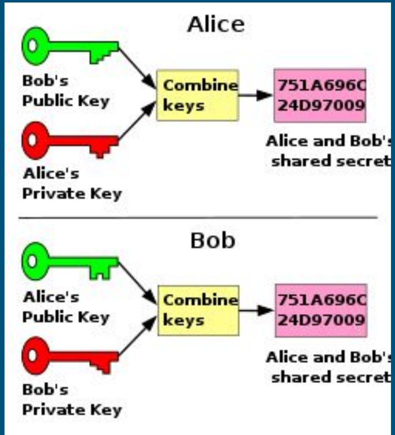


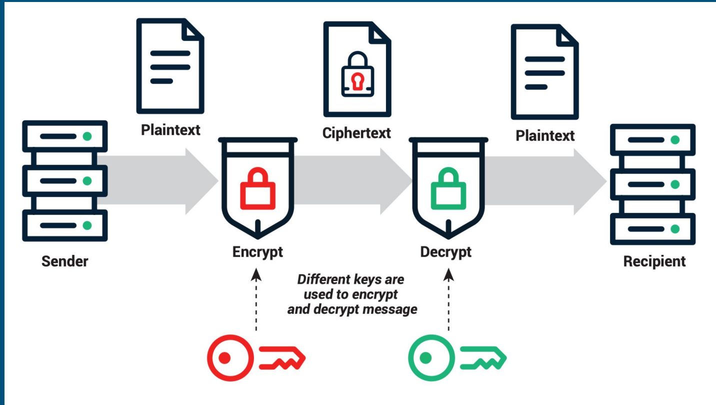


Asymmetric Ciphers

- Relies on both a public and private key
  - This way, there isn’t a need to share a secret key
  - Usually slower than symmetric ciphers
  - Used over the internet where sending keys probably isn’t a great idea
- Elliptic curves

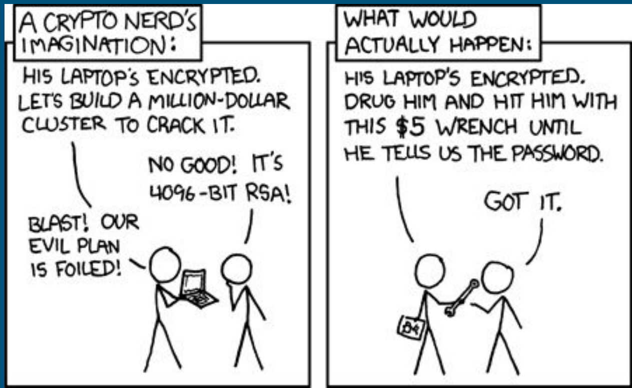






Side Channel Attacks

- It’s often a lot easier to exploit the software or people rather than the cipher
- Randomness is hard
  - We can deduce the keys sometimes just based on the time
  - Other ways include acoustic, electromagnetic, and power consumption
- Social engineering
  - Often the people screw up, not the math


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Thanks for Coming!