Meets monthly

discord.defcon908.org

defcon908.org

meetup.com/defcon908

@defcon908

Organizers

Dan Sherry

Organizer

dan@defcon908.org

@netbroom

Jeremy Chisamore

Organizer

jeremy@defcon908.org

@chazb0t

Ben Smith

Advisor

ben@defcon908.org

/in/bensmith83/

Matt K

Advisor

matt@defcon908.org

Call for Talks

30 minutes + Q&A

- Technical
- Career
- Entrepreneurship or side projects
- “War stories” or research
- Demos
- Workshops

Introductions

2 minutes each - 15 minutes

Talk

Disclaimer: photos may be taken

Encryption

Dan Sherry

Dan Sherry

- Coded for 15+ years
- BS in Cybersecurity
- Incident response, security engineering 2013 - 2017
- Founded Pulsedive in 2017
- Coded from scratch:
  - Threat intelligence platform
  - JARM TLS fingerprinting
  - Web authentication
  - App-based MFA
  - LetsEncrypt cert issuance
- **I still have to Google stuff**
  - What algo to use and when?
  - How to connect with socket?
  - How to open PDF?

Pulsedive®
Community

GUNAX LBH

In cryptography, encryption is

the process of transforming information in a way that, ideally, only authorized parties can decode.

- Wikipedia

Basic Terms

- Encryption obfuscates a **plaintext** (the original message) using a **key** (or “secret”) to create a **ciphertext** such that the message cannot be read without the key.
- The ciphertext can be **decrypted** using a **key**
- Symmetric encryption - same key to encrypt/decrypt
- Asymmetric encryption - **public key** to encrypt and **private key** to decrypt
- Secure keys are **random**

Early Methods

Earliest Ciphers

- Clay tablets in Mesopotamia from 1500 BC to encrypt a craftsman’s recipe for pottery glaze
- Early Hebrew Atbash cipher in ancient Israel from 500-600 BC

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

- Mlecchita vikalpa (from the Kamasutra) - India between 300-400 BC
  - “The art of understanding writing in cypher, and the writing of words in a peculiar way.”
  - Later commentaries on the Kamasutra described several methods using basic ciphers
- Great timeline: ibm.com/think/topics/cryptography-history

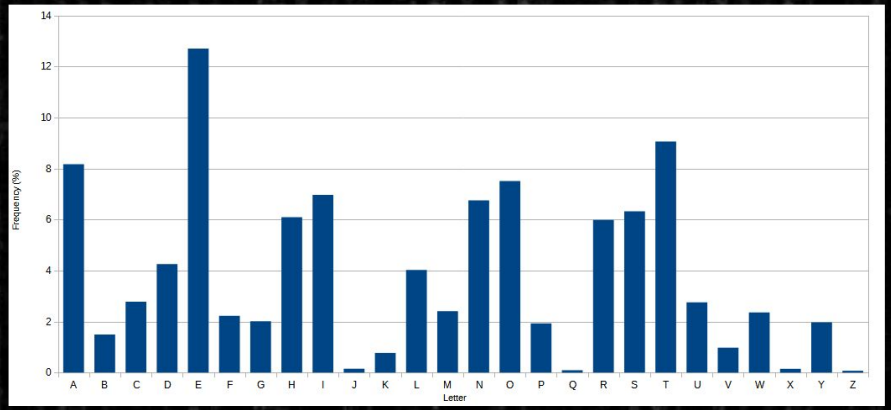
Caesar Cipher

- Used by Julius Caesar to protect messages of military significance
- Used by the Confederates, and by others into the 20th century
- Simple offset of letters
- “ROT13” uses offset 13

Plain	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
Cipher	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

Breaking the Caesar Cipher

- Brute force
  - Key range is only 1-26
- Frequency analysis
  - Initially developed by Al-Kindi around 800-900 AD in present-day Iraq
  - Some letters in English appear more often (eg: A, E)
  - Combinations of letters more common (eg: ING, EA)



Enigma

Invented by the Germans at the end of WWI, used by Nazis in WWII

Initially replicated & broken by Polish ~1932

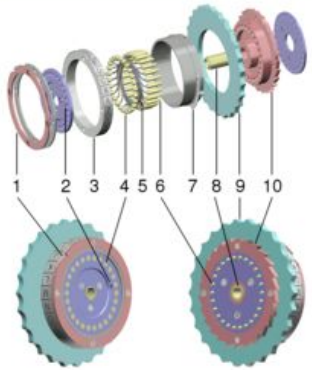
1939 - Polish contributed materials to British effort as war became imminent and Enigma became more complex

Broken by Alan Turing & other British codebreakers in Bletchley Park ~1940

Movie - The Imitation Game

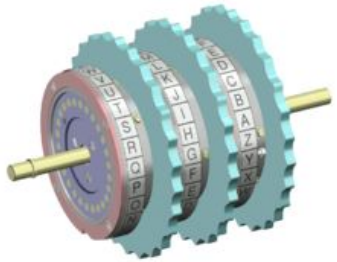
Enigma

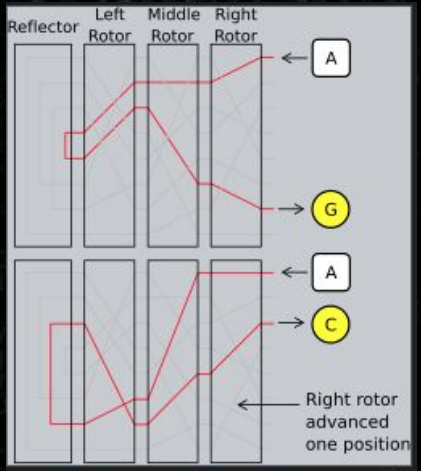
Exploded view of an Enigma rotor



1. notched ring
2. marking dot for "A" contact
3. alphabet tyre
4. plate contacts
5. wire connections
6. pin contacts
7. spring-loaded ring adjusting lever
8. hub
9. finger wheel
10. ratchet wheel

Three rotors in sequence





The scrambling action of the Enigma rotors shown for two consecutive letters — current is passed into set of rotors, around the reflector, and back out through the rotors again. Note: The greyed-out lines represent other possible circuits within each rotor, which are hard-wired to contacts on each rotor. Letter A encrypts differently with consecutive key presses, first to G, and then to C. This is because the right hand rotor has stepped, sending the signal on a completely different route.

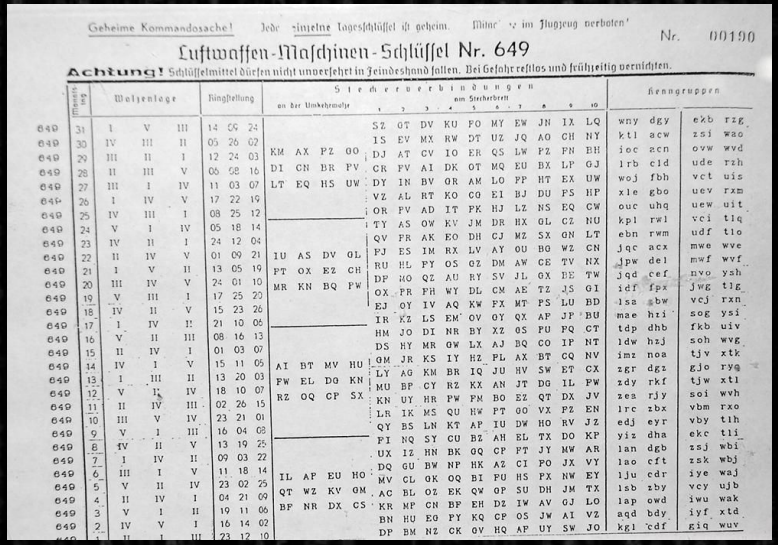
Enigma

Symmetric encryption using rotors, rings, plugboards, set according to “setting sheets” by date

Setting sheets include wheel/rotor order, ring settings, plug connections, starting positions of rotors

Enigmas on either end must have same configuration for encryption/decryption

Wikipedia: For example, the settings for the 18th day of the month in the German Luftwaffe Enigma key list number 649 were as follows:


Geheime Kommandosache! Jede einzelne Tagesschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Monatstag	Walzenlage	Ringstellung	Steckerverbindungen an der Umkehrwalze	Steckerverbindungen am Steckerbrett 1 2 3 4 5 6 7 8 9 10	Spruchgruppen
649	31 I V III	14 06 24	KM AX FZ GO	SZ GT DV KU FO MY EW JN IX LQ	wny dgy ekb rzg
649	30 IV III II	05 26 02	DI CN BR PV	IS EV MX RW DT UZ JQ AO CH NY	ktl acw zsi wao
649	29 III II I	12 24 03	LT EQ HS UW	DJ AT CV IO ER QS LW PZ FN BH	ioc acn ovw wvd
649	28 II III V	06 08 16		CR FV AI DK OT MQ EU BX LP GJ	lrb cld ude rzh
649	27 III I IV	11 03 07		DY IN BV OR AM LO FP HT EX UW	woj fbh vct uis
649	26 I IV V	17 22 19		VZ AL RT KO CQ EI BJ DU FS HP	xle gbo uev rxm
649	25 IV III I	08 25 12		OR FV AD IT PK HJ LZ NS EQ CW	ouc uhq uew uit
649	24 V I IV	05 18 14		TY AS OW KV JM DR HX GL CZ NU	kpl rwl vci tlq
649	23 IV II I	24 12 04	IU AS DV GL	QV FR AK EO DH CJ MZ SX GN LT	ebn rwm udf tlo
649	22 II IV V	01 09 21	PT OX EZ CH	FJ ES IM RX LV AY OU BQ WZ CN	jqc acx mwe wve
649	21 I V II	13 05 19	MR KN BQ PW	RU HL FY OS QZ DM AW GE TV NX	jpw del mwf wvf
649	20 III IV V	24 01 10		DP HO QZ AU RY SV JL GX BE TW	jqd cef nvo ysh
649	19 V III I	17 25 23		OX FR FH WY DL CM AE TZ JS GI	idf fpx jwg tlg
649	18 IV II V	15 23 26		EJ OY IV AQ KW FX MT PS LU BD	lsa zbw vcj rxn
649	17 I IV II	21 10 06		IR KZ LS EM OV OY QX AP JP BU	mae hri soq ysi
649	16 V II III	08 16 13	AI BT MV HU	HM JO DI NR BY XZ GS PU PQ CT	idp dhb fkb uiv
649	15 II IV I	01 03 07	FW EL DQ KN	DS HY MR GW LX AJ BQ CO IP NT	ldw hzj soh wvg
649	14 IV I V	15 11 05	RZ OQ CP SX	GM JR KS IY HZ PL AX BT GQ NV	imz noa tjv xtk
649	13 I III II	13 20 03		LY AG KM BR IQ JU HV SW ET CX	zgr dgz gjo ryq
649	12 V II IV	18 10 07		MU BF CY RZ KX AN JT DG IL PW	zdy rkf tjw xtl
649	11 II IV III	02 26 15		KN UY HR FW FM BO EZ QT DX JV	zea rjy soi wvh
649	10 III V IV	23 21 01		LR IK MS QU NW PT GO VX FZ EN	lrc zbx vbm rxo
649	9 V I III	16 04 08		QY BS LN KT AP IU DW HO RV JZ	edj eyr vby tlh
649	8 IV II V	13 19 25	IL AF EU HO	FI NQ SY CU BZ AH EL TX DO KP	yiz dha ekc tli
649	7 I IV II	09 03 22	QT WZ KV GM	UX IZ HN BK OQ CP FT JY MW AR	lan dgb zsj wbi
649	6 III I V	11 18 14	BP NR DX CS	DQ GU BW NP HK AZ CI PO JX VY	lao cft zsk wbj
649	5 V II IV	23 02 25		MV CL GK OQ BI FU HS FX NW EY	lju cdr iye waj
649	4 II IV I	04 21 09		AC BL OZ EK QW QP SU DH JM TX	lsb zby vcy ujb
649	3 V I II	19 11 06		KR MP CN BP EH DZ IW AV GJ LO	lap owd iwu wak
649	2 IV V I	16 14 02		BN HU EQ FY KQ CP OS JW AI VZ	aqd bdy iyf xtd
649	1 II I III	23 12 10		DP BM NZ GK OV HQ AP UY SW JO	kgi cdf giq wuv

- Wheel order: IV, II, V
- Ring settings: 15, 23, 26
- Plugboard connections: EJ OY IV AQ KW FX MT PS LU BD
- Reconfigurable reflector wiring: IU AS DV GL FT OX EZ CH MR KN BQ PW
- Indicator groups: lsa zbw vcj rxn

The Information Age

Boolean Algebra

Branch of Discrete Mathematics

- Logic, set theory, relational algebra, etc

Invented by George Boole in the 1800s

- English mathematician, philosopher and logician

Logical operations on binary values

- True and False (0 and 1)

Used heavily with computers and programming

Boolean Algebra

Logical operations on true/false values

- AND (∧): both must be True
  - T AND F = F
- OR (∨): either must be True
  - T OR F = T
- NOT (¬): negates value
  - -T = F
- XOR (⊕): Exactly one must be True
  - T XOR T = F

Boolean Algebra - Examples

T OR F = ?

(T OR T) AND T = ?

(F OR F) AND F = ?

(T XOR T) OR T = ?

((T AND T) AND F) OR (T XOR F) = ?

Truth Tables

AND	T	F
T	T	F
F	F	F

OR	T	F
T	T	T
F	T	F

Wait a second...

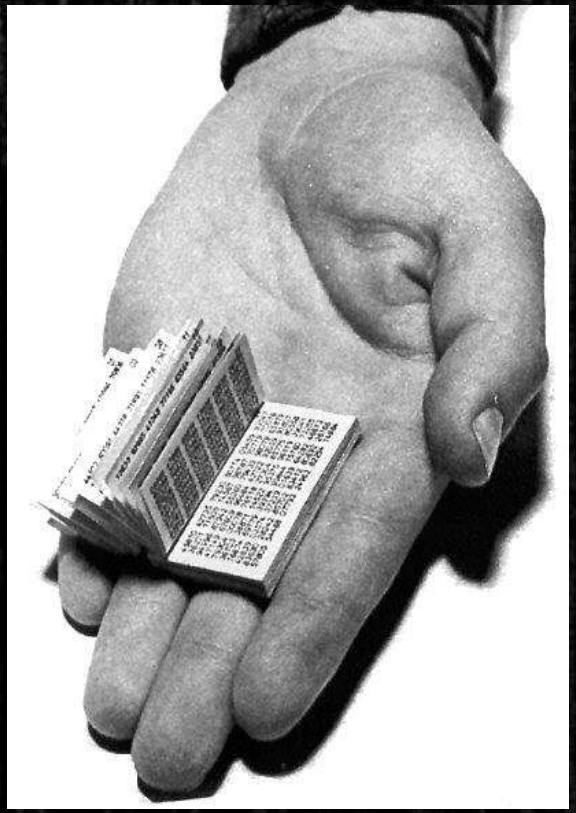
XOR	T	F
T	F	T
F	T	F

XOR is reversible

```
1 0 0 1 0 1 1 0 1   PLAINTEXT
0 1 0 0 1 1 0 1 1   KEY
1 1 0 1 1 0 1 1 0   CIPHERTEXT
```

One-Time Pad

- Encrypts a plaintext with a single pre-shared key
- Initially invented in 1882 by Frank Miller
- Electrical one-time pad patented in 1919 by Gilbert Vernam (AT&T) using XOR
- Used by KGB, NSA, Moscow-Washington hotline (red telephone) est. in 1963
- **Unbreakable!** If:
  - Key is as long as plaintext or longer
  - Key is random
  - Key is not reused
  - Key is kept secret




WE
DID IT!

One-Time Pad Limitations

Secure if:

- Key is as long as plaintext or longer
- Key is random
- Key is not reused
- Key is kept secret

OK fine

I want to encrypt my CVS receipt :(

How do I do that? :(

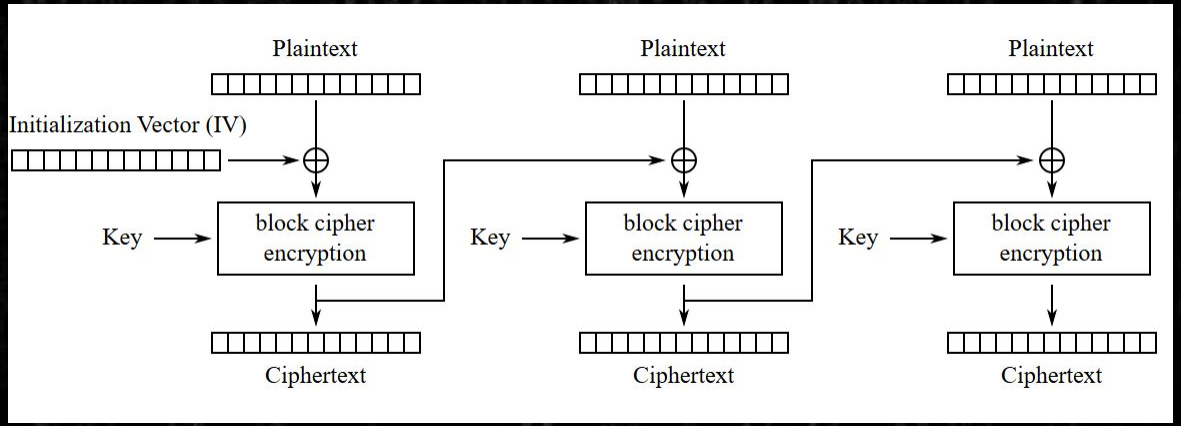
How do I send it to my friend? :(

Block Cipher

Encrypts fixed-length groups of bits

- Electronic codebook mode (ECB) - encrypt/decrypt each block independently
- Cipher block chaining (CBC)
  - First block is random bits called an initialization vector (IV)
  - XOR'd with first plaintext block and encrypted
  - Resulting ciphertext block used as IV for next block

Solves message length problem



Stream Cipher

Inspired by one-time pad

- Gilbert Vernam’s (AT&T) idea was to use “one-time tape” but initial designs meant key would be re-used because the tape was a loop

Encrypts plaintext bit-by-bit

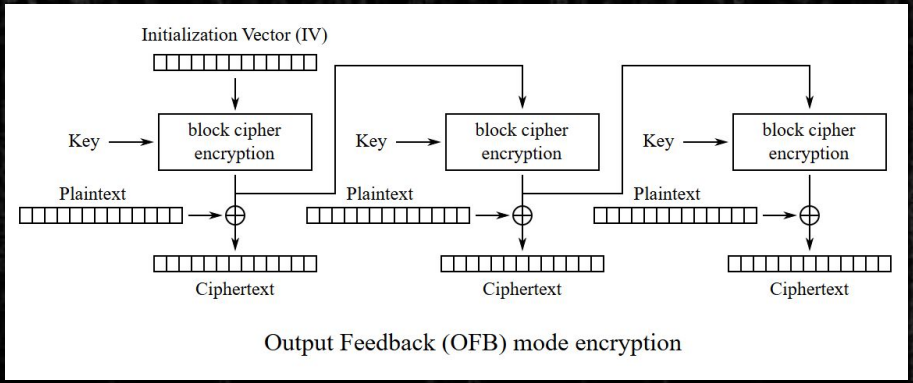
- Generates keystream to combine with plaintext bits and produce ciphertext

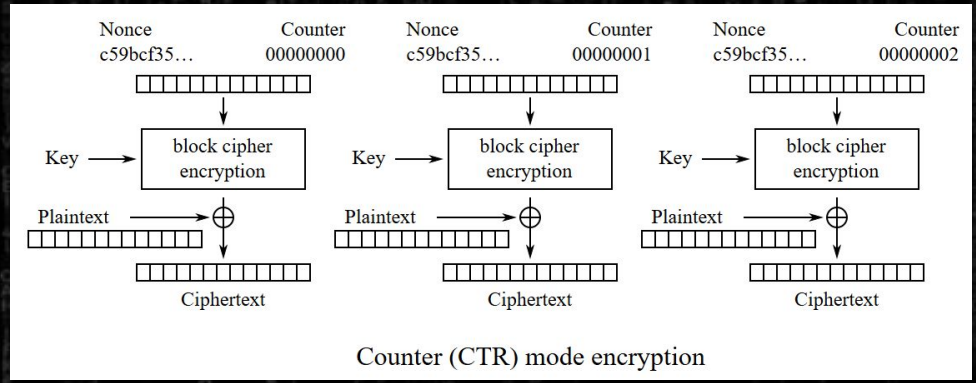
Solves encrypting data of unknown length

Stream Cipher

Block ciphers can be converted to stream ciphers

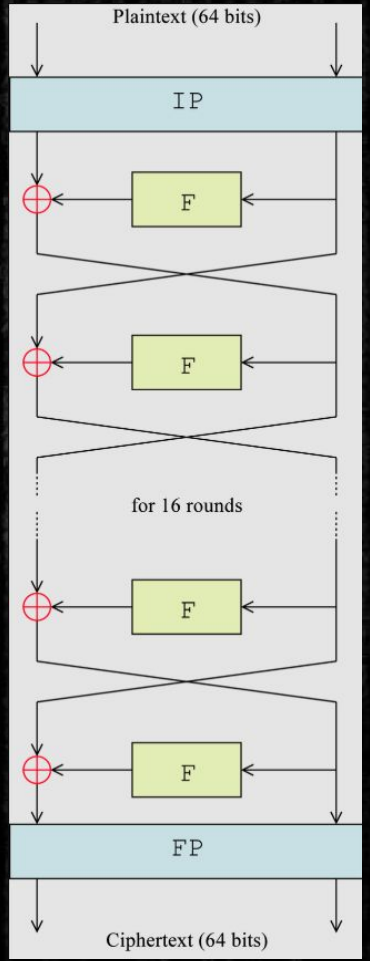
- Output feedback mode (OFB)
  - Generates keystream blocks, XORed with plaintext blocks to get ciphertext
- Counter mode (CTR)
  - Generates keystream by encrypting a “counter” for each block





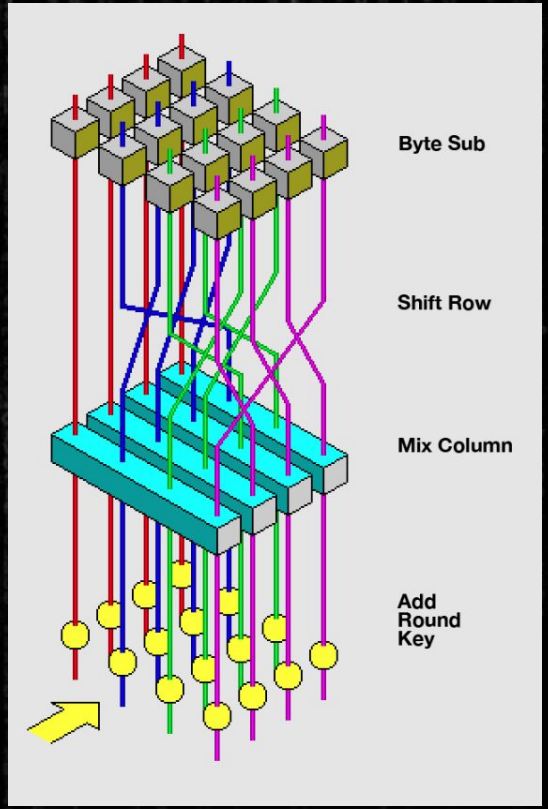
Data Encryption Standard (DES)

- 1970’s - NIST solicited proposals for encryption standard
- Selected an algorithm developed at IBM
  - Based on earlier Lucifer cipher designed by Horst Feistel
- Block cipher
  - Block size - 64 bits
  - Key size - 64 bits ***but only 56 are used***
- Not secure
  - Short key length = brute force
  - Additional cryptanalysis attacks and vulnerabilities
- Triple DES (3DES)
  - Attempts to improve security by applying DES 3 times each block
  - Recent CVE in 2016 affects both DES and 3DES - CVE-2016-2183



Advanced Encryption Standard (AES)

- 1997 - NIST seeks successor to DES
- 2000 - NIST selected Rjindael cipher
- Now an official standard and used heavily today
- Block cipher
  - Block size - 128 bits
  - Key size - 128, 192, or 256 bits
  - Modes: CBC, CTR, ECB, GCM, etc
- Still secure - no known practical attacks
  - Side channel attacks - attacks on hardware/software that leak data
- AES-256 is considered to be “quantum resistant”



Diffie-Hellman Key Exchange

- Solved: How does each party get the key securely?
- 1976 - Ralph Merkle, Whitfield Diffie, and Martin Hellman developed key exchange protocol
- Can share symmetric key over untrusted medium securely
- Uses asymmetric encryption
- Secure
  - Quick to generate key
  - Slow to brute force without knowing secrets

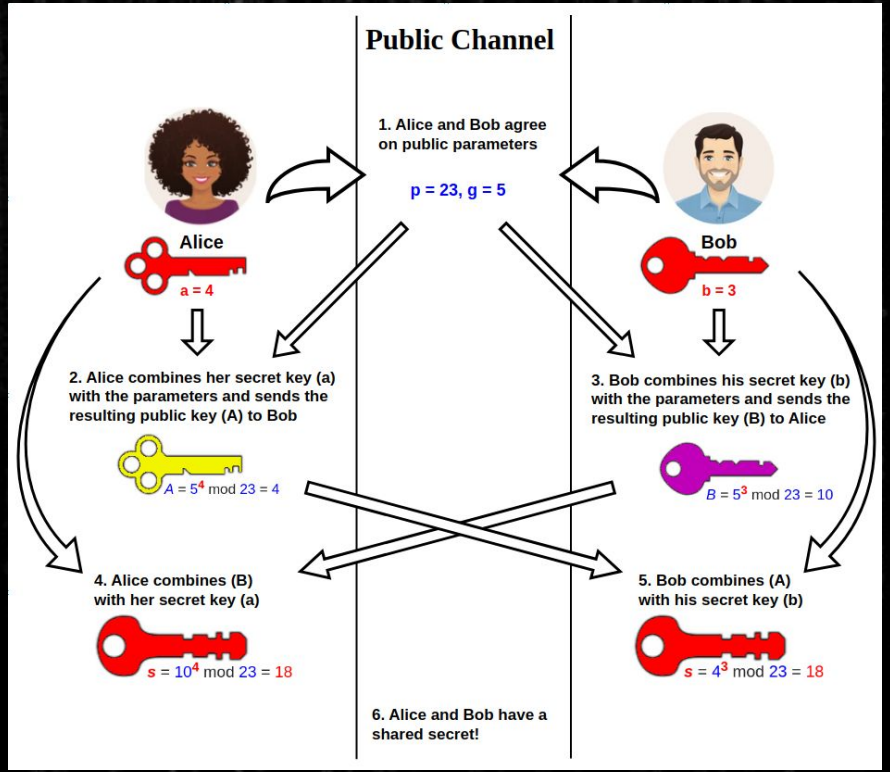
Diffie-Hellman Key Exchange

How?

1. Each party generates a public and private key using shared parameters + secret
2. Each party encrypts their secret with the other's public key and returns
3. Each party decrypts with their private key and arrives at the same result

Secure

- Quick to generate key
- Slow to brute force without knowing secrets



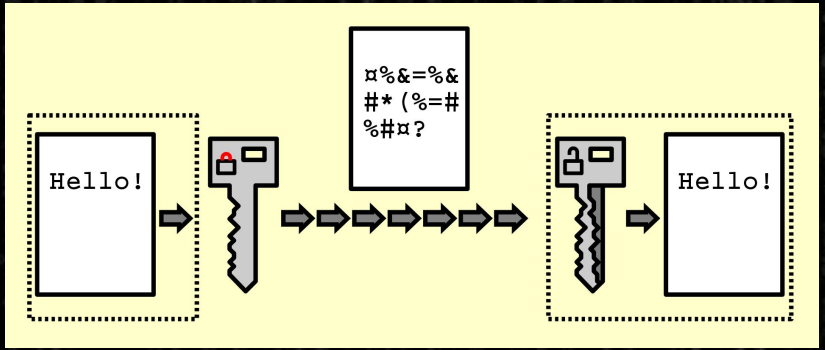
RSA Encryption

- 1977 - developed by Ron Rivest, Adi Shamir, Leonard Adleman at MIT
- Like Diffie-Hellman, RSA is based on modular exponentiation
- Uses random large prime numbers to generate public key for encryption and private key for decryption
- Can be used for message signing
  - Digital signature generated using private key
  - Confirms to receiver that message was not tampered with

Bridging the Gap

Encryption vs Hashing

Encryption is reversible.

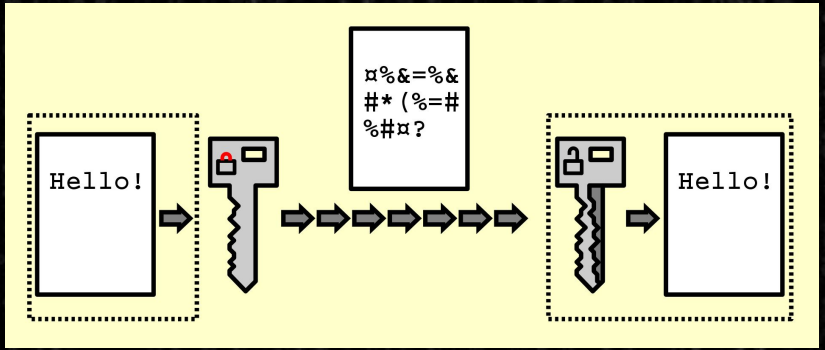


Hashing: 1 input = 1 output (digest)

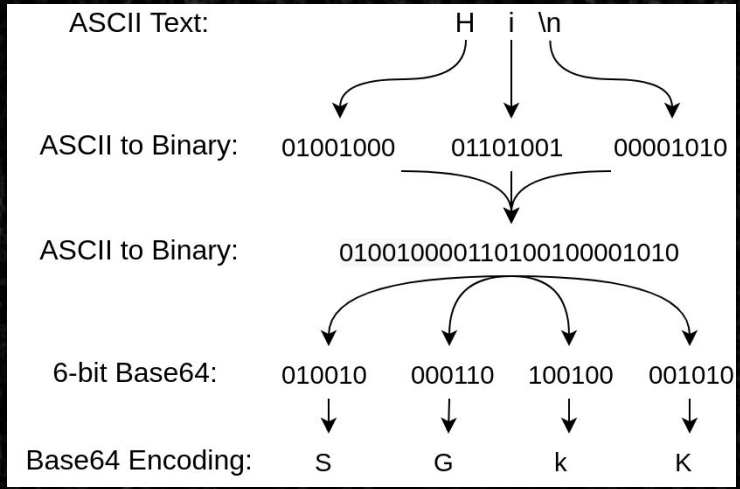
Fox	Hash function	DFCD3454
The red fox runs across the ice	Hash function	52ED879E
The red fox walks across the ice	Hash function	46042841

Encryption vs Base64

Encryption requires a key, only for authorized parties.



Base64 can be decoded by anyone.



Technologies you've heard of:

SSH	RSA (signing), Diffie-Hellman, AES
TLS (HTTPS)	RSA, Diffie-Hellman, AES
PGP (Email)	RSA
Signal Protocol & WhatsApp	Extended Triple Diffie-Hellman (X3DH), AES-256
Tor	Diffie-Hellman, AES
Full Disk Encryption (FDE)	AES
Encryption-at-rest	AES

Rolling Your Own Crypto

DO NOT ROLL YOUR OWN CRYPTO.

Node.js	native	node:crypto
Golang	native	crypto package
PHP	native	OpenSSL functions
Other languages		OpenSSL - included w/ most Linux systems
		Third-party package/library

GUNAX LBH

7 21 14 1 24 12 2 8 + 13 20 8 1 14 11 25 15 21

THANK YOU

Call for Volunteers