Cryptographic Primitives

What is Cryptography?

> “Communication in the presence of adversaries” - Ron Rivest

LoliRock

2016 TV-Y 2 Seasons

A teenager with a beautiful voice becomes a pop star but discovers she has powers that come from a magical realm where she's a lost princess.

Starring: Kazumi Evans, Kelly Sheridan, Vincent Tong
Genres: TV Shows, Kids' TV, Kids' TV for ages 5 to 7

MY LIST

Encryption: Caesar Cipher

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
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

QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

Encryption: One-Time Pad

- Use a different shift at every position!

Hf{#Fth'B2

0 1 2 3 4 5 6 7 8 9

Hey Bob :)

0 1 2 3 4 5 6 7 8 9

Encryption: One-Time Pad

- “Hey Bob :)” >> (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) = “Hf{#Fth'B2”
- “Hey Bob :(” >> (0, 1, 2, 3, 4, 5, 6, 7, 8, 10) = “Hf{#Fth'B2”
- “Attack now” >> (7, -14, 7, -62, -29, 9, 72, -71, -45, -69) = “Hf{#Fth'B2”

- Information-theoretic security

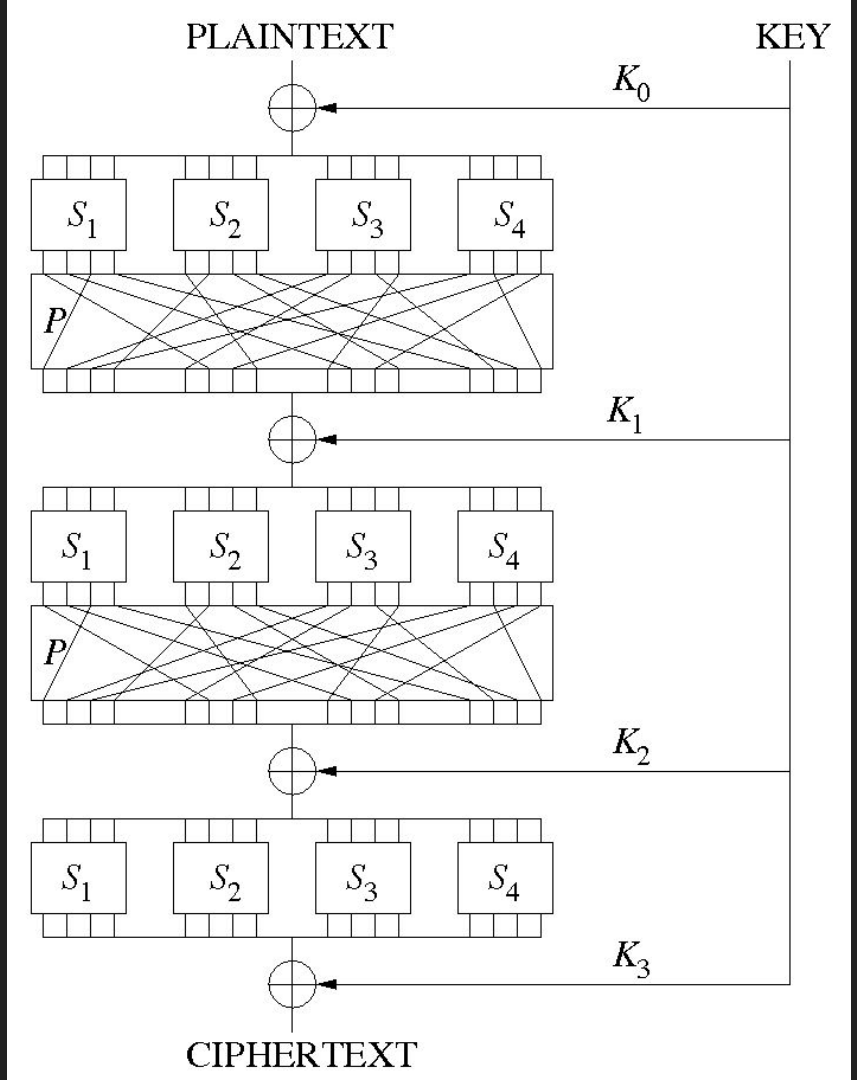
Encryption: Substitution

Caesar Cipher:

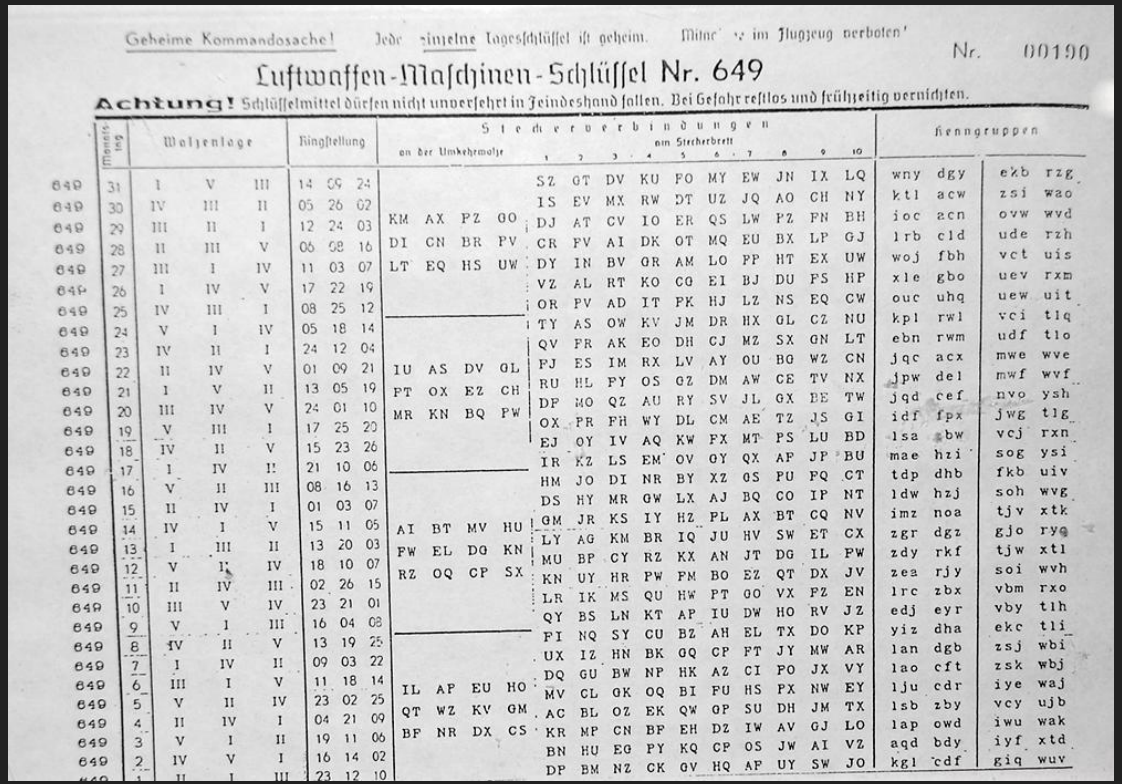
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XYZABCDEFGHIJKLMNOPQRSTUVW

Advanced Encryption Standard:

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT

Key Exchange



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

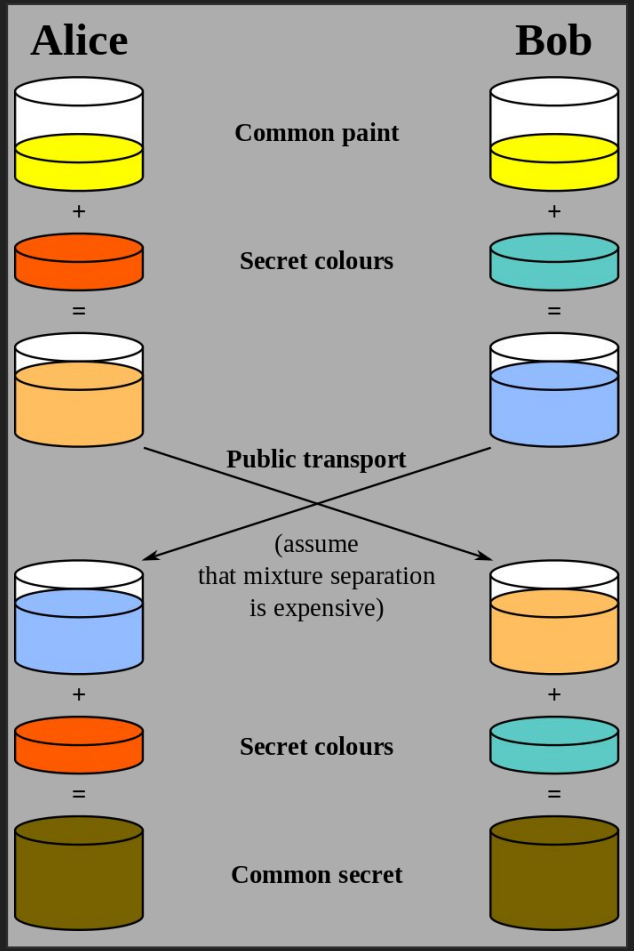
Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

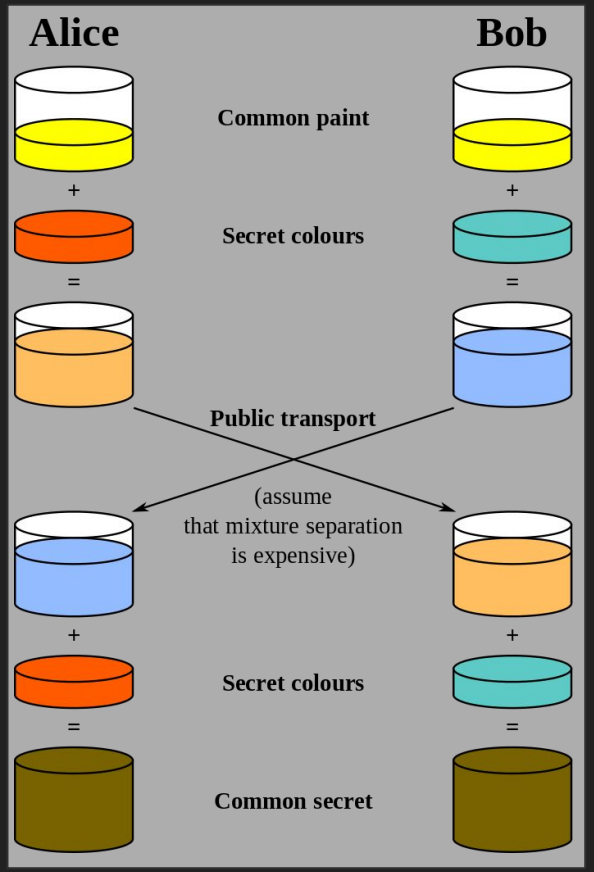
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

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

Key Exchange



Key Exchange: Diffie-Hellman



Alice

Bob

$p = 23,$
$g = 5$

$a = 6$

$b = 15$

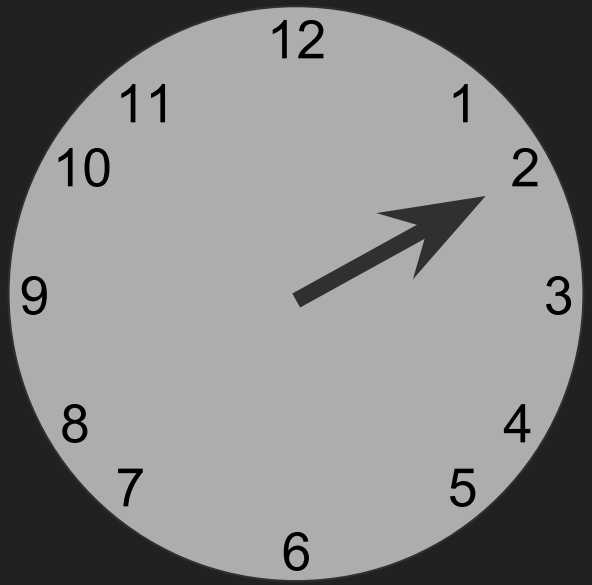
$A = g^a = 5^6 = 8 \pmod{23}$

$B = g^b = 5^{15} = 19 \pmod{23}$

Modular Arithmetic

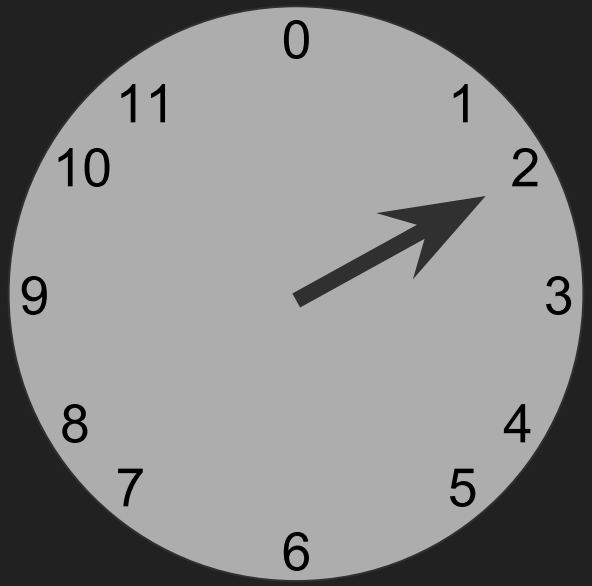
Clock Arithmetic

8 + 6 = 2 (mod 12)



Modular Arithmetic

Clock Arithmetic

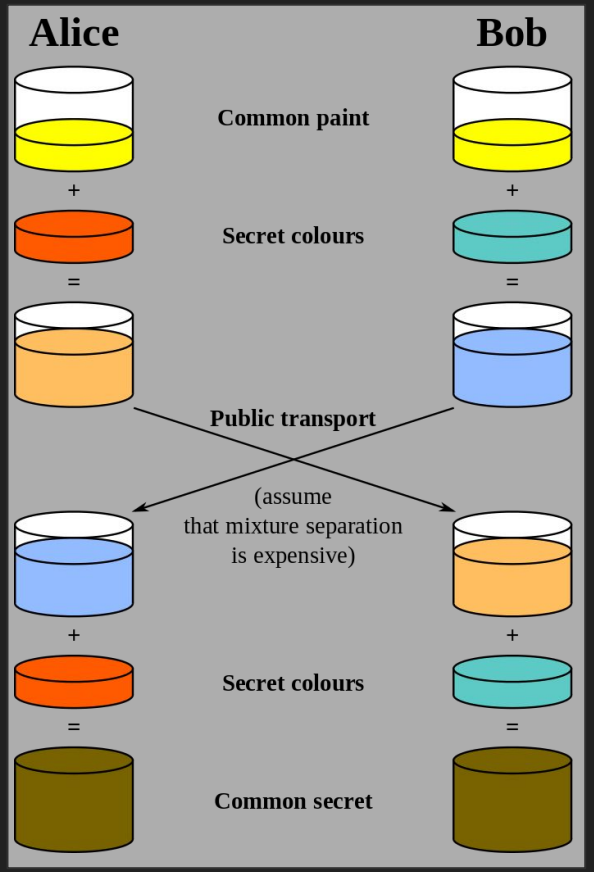


8 + 6 = 2 (mod 12)

6 * 2 = 0 (mod 12)

$a = b \pmod{n}$
if and only if
$a - b = k \cdot n$ for some k
(a and b differ by a multiple of n)

Key Exchange: Diffie-Hellman



Alice

Bob

$p = 23,$
$g = 5$

$a = 6$

Assume that discrete logs are expensive

$b = 15$

$A = g^a = 5^6 = 8 \pmod{23}$

$B = g^b = 5^{15} = 19 \pmod{23}$

$k = B^a = 19^6 = 2 \pmod{23}$

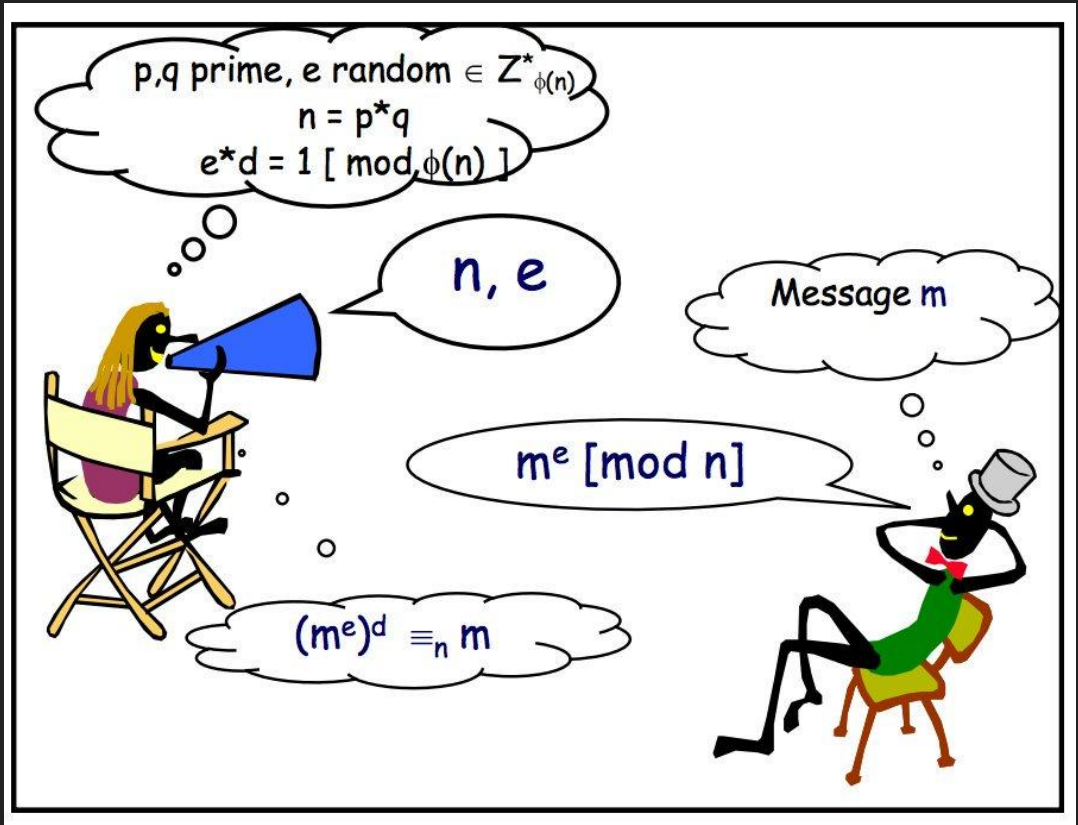
$k = A^b = 8^{15} = 2 \pmod{23}$

$k = g^{ab} = g^{ba}$

Public Key Encryption

- Use separate keys for encryption and decryption
- Anyone can use my public key to encrypt a message for me
- Only I have the private key for decryption

Public Key Encryption: RSA

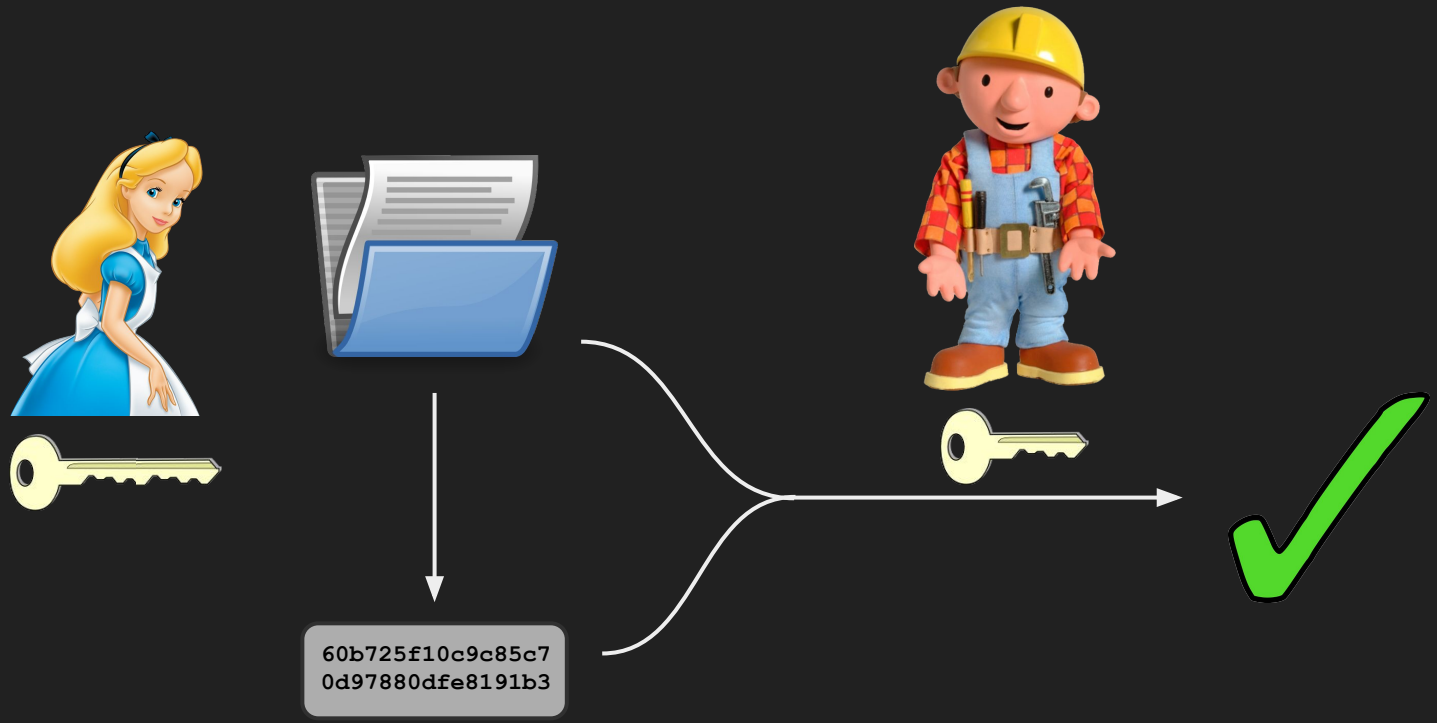


Enc(m) = m^e

Dec(c) = c^d

Dec(Enc(m)) = m (mod n)

Digital Signatures



Digital Signatures: RSA

RSA Encryption: Dec(Enc(m)) = m

RSA Signatures: Enc(Dec(m)) = m

Sign(m) = Dec(m) = m^d

Verify(s) = Enc(s) = s^e

e is the public key, d is the private key

Digital Signatures: Forging RSA

- Find m, s such that Verify(s) = $s^e = m$
- m will always be a valid signature for m^e
- Existential forgery

Homework

- Forge an RSA signature against a network service
- `nc 54.86.3.162 1977`
- For extra credit, forge the particular message 1337

Tips

- **Don’t hesitate to ask questions! (Slack, email, etc)**

Homework grading

- Send an email to cm7bv@virginia.edu with the subject “MST Assignment 6 - <YOUR_UVA_ID>”
  - eg: “MST Assignment 6 - cm7bv”
- Include a brief (1-paragraph) description of what you did and how it went

Hash Functions

Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	2.9G	**2016.2**	25cc6d53a8bd8886fcb468eb4fbb4cdfac895c65
Kali Linux 32 bit	ISO	Torrent	2.9G	**2016.2**	9b4e167b0677bb0ca14099c379e0413262eefc8c
Kali Linux 64 bit Light	ISO	Torrent	1.1G	**2016.2**	f7bdc3a50f177226b3badc3d3eafcf1d59b9a5e6
Kali Linux 32 bit Light	ISO	Torrent	1.1G	**2016.2**	3b637e4543a9de7ddc709f9c1404a287c2ac62b0
Kali Linux 64 bit e17	ISO	Torrent	2.7G	**2016.2**	4e55173207aef7ef584661810859c4700602062a
Kali Linux 64 bit Mate	ISO	Torrent	2.8G	**2016.2**	bfaeaa09dab907ce71915bcc058c1dc6424cd823
Kali Linux 64 bit Xfce	ISO	Torrent	2.7G	**2016.2**	e652ca5410a44e4dd49e120befdace38716b8980
Kali Linux 64 bit LXDE	ISO	Torrent	2.7G	**2016.2**	d8eb6e10cf0076b87abb12eecb70615ec5f5e313
Kali Linux armhf	Image	Torrent	0.7G	**2016.2**	7aec28a2aa7f303467d29d7e3cf38fd372aefe4c
Kali Linux armel	Image	Torrent	0.7G	**2016.2**	6b90d5a7f8d2627016e63caf5b895f7ca814c6c0

Hash Functions

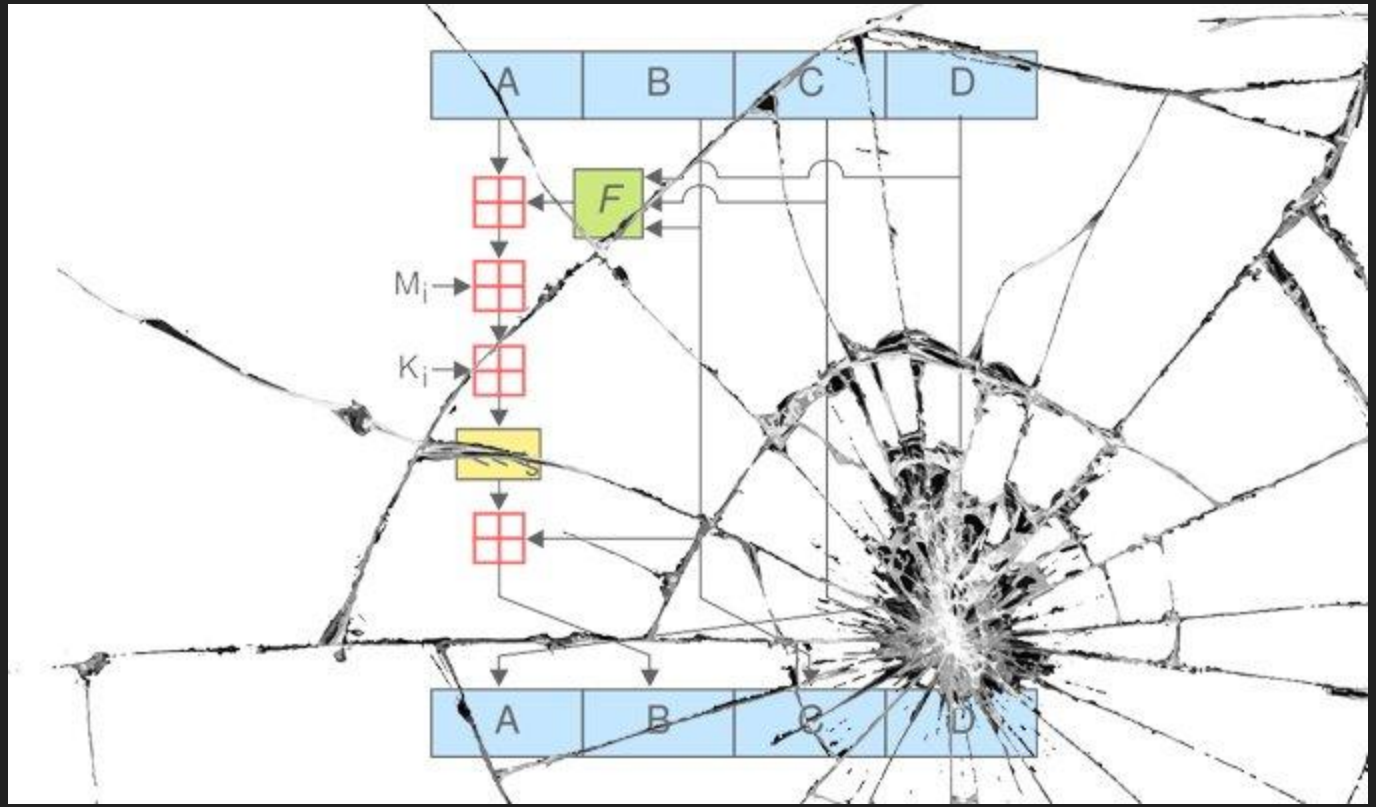
Password hashing

Preimage resistance

Hash Functions

- Hash then sign
  - sig = Sign(m) = (Hash(m))^d
  - Verify that sig^e = Hash(m)
- Collision resistance

#SHAttered



Further Reading

- AES: The Making of a New Encryption Standard (https://www.sans.org/reading-room/whitepapers/vpns/aes-making-encryption-standard-740)
- Handbook of Applied Cryptography: Chapter 1 (http://cacr.uwaterloo.ca/hac/)
- Udacity cs387: Applied Cryptography by Dave Evans (https://www.udacity.com/course/applied-cryptography--cs387)
- Dan Boneh’s Cryptography Coursera Course (https://www.coursera.org/learn/crypto)