Cryptography Fundamentals for Java and .NET Developers

Introduction

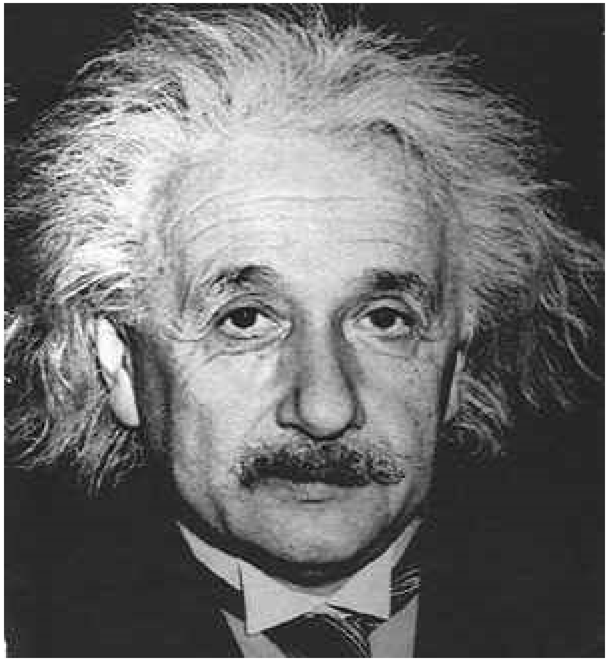
Michael L Perry
qedcode.com
@michaellperry

pluralsight
hardcore dev and IT training

Target

Snapchat

NSA

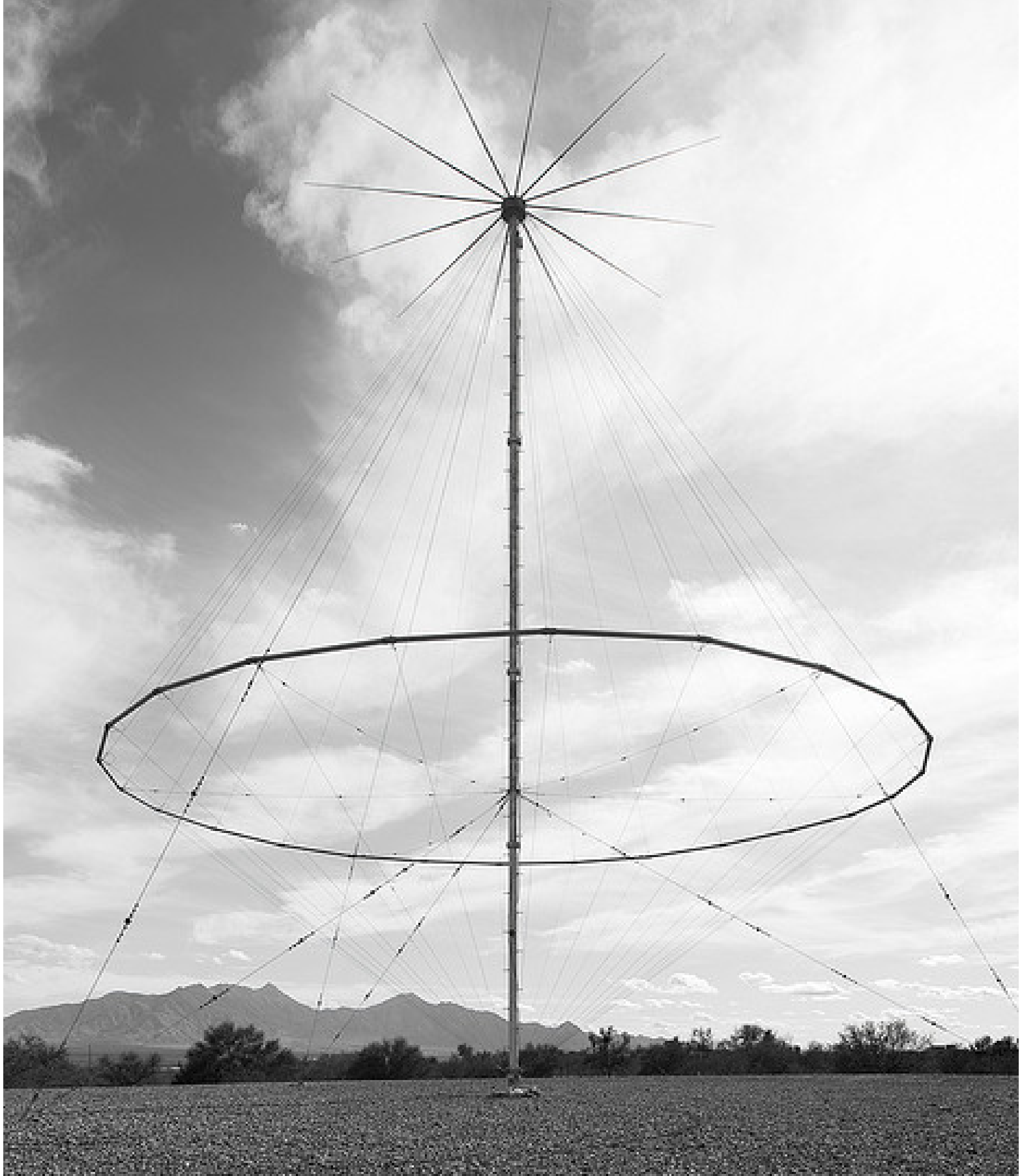


History of Cryptography

- Three greatest advances
- Today’s methods
- Exciting future

The Weakest Link

Humans



The Cornet Project

Recordings of Shortwave Numbers Stations

Shortwaveology.net

One-Time Pad

MAMPE BVQDI JQORJ WRELZ

12 0 12 15 4 1 21 16 3 8 9 16 14 17 9 22 17 4 11 25

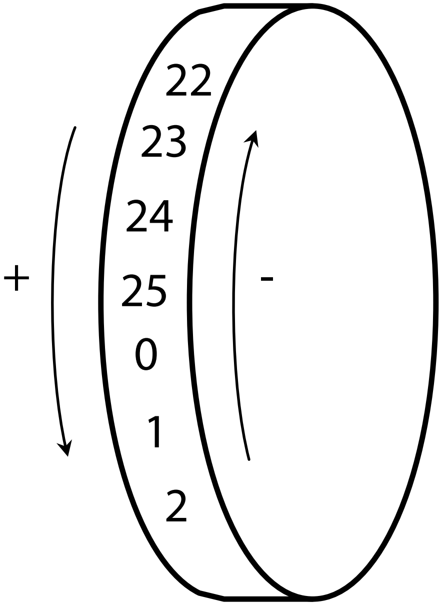
DELIV ERYAT NINET HIRTY

3 4 11 8 21 4 17 24 0 19 13 4 19 7 8 7 8 17 19 24

PEXXZ FMODB WYBVC DZVEX

15 4 23 23 25 5 12 14 3 1 22 24 1 21 2 3 25 21 4 23

Addition Modulo 26



Possible Keys

CGPJ QYXT

2 6 15 9 16 24 23 19

ASDF JKLP

0 18 3 5 9 10 11 15

RCDV DYUP

17 2 3 21 3 24 20 15

COME HOME

2 14 12 4 7 14 12 4

LEMO NADE

11 4 12 14 13 0 3 4

Pseudo Random Numbers

$$(Ax_0 + B) \bmod 2^{64} = x_1$$

3,227,678,411,623,578,827	9	J
3,385,237,196 ,860,930,252	16	Q
1,905,768,108 ,648,866,984	10	K
250,722,988 ,989,761,836	22	W
739,326,635 ,180,224,684	21	V
2,072,715,979 ,080,927,912	9	J
4,241,563,340 ,079,199,532	14	O
206,026,408 ,329,146,540	16	Q

Entropy

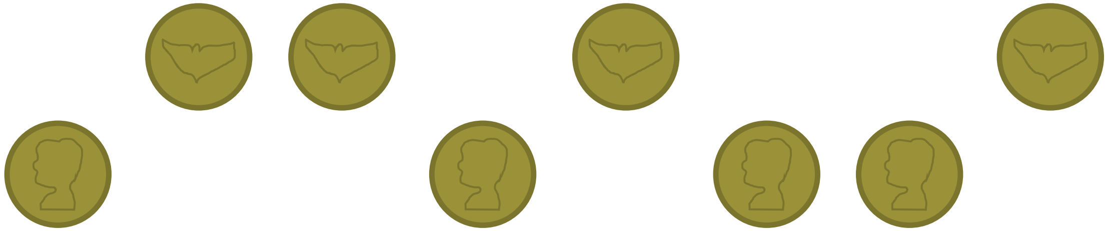
Claude E. Shannon

A Mathematical Theory of Communication

1948

Information theory

Bit



0 1 1 0 1 0 0 1

One-Time Pad

MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ
12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25
DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY
3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24
PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX
15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23
MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ
12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25
DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY
3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24
PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX
15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23
MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ
12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25
DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY
3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24
PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX
15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23
MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ
12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25
DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY	DELIV	ERYAT	NINET	HIRTY
3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24	3 4 11 8 21	4 17 24 0 19	13 4 19 7 8	7 8 17 19 24
PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX	PEXXZ	FMODB	WYBVC	DZVEX
15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23	15 4 23 23 25	5 12 14 3 1	22 24 1 21 2	3 25 21 4 23
MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ	MAMPE	BVQDI	JQORJ	WRELZ
12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25	12 0 12 15 4	1 21 16 3 8	9 16 14 17 9	22 17 4 11 25

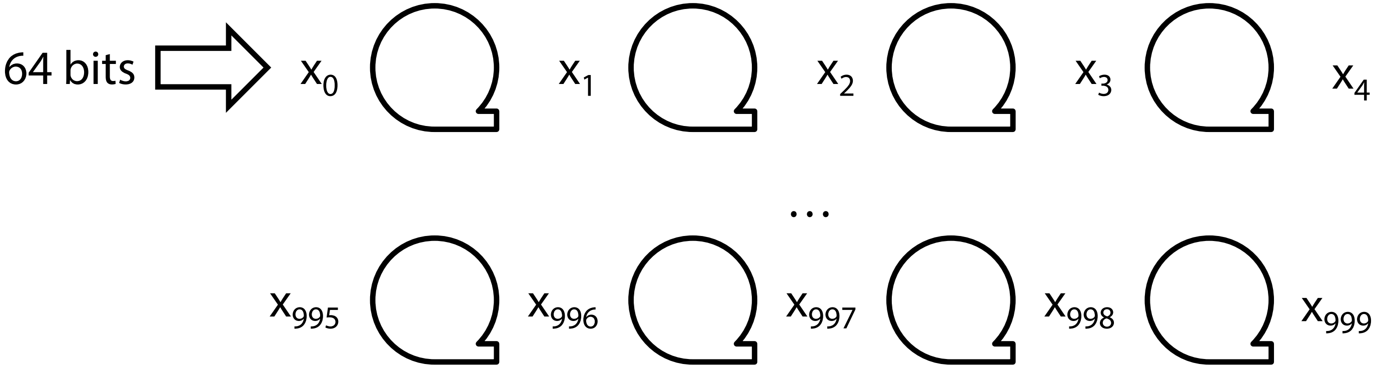
One-Time Pad

$$\log_2(26) = 4.7$$

(that is, $2^{4.7} = 26$)

$$1{,}000 \text{ x } 4.7 = 4{,}700$$

Pseudo-Random Pad



64 bits (at most)

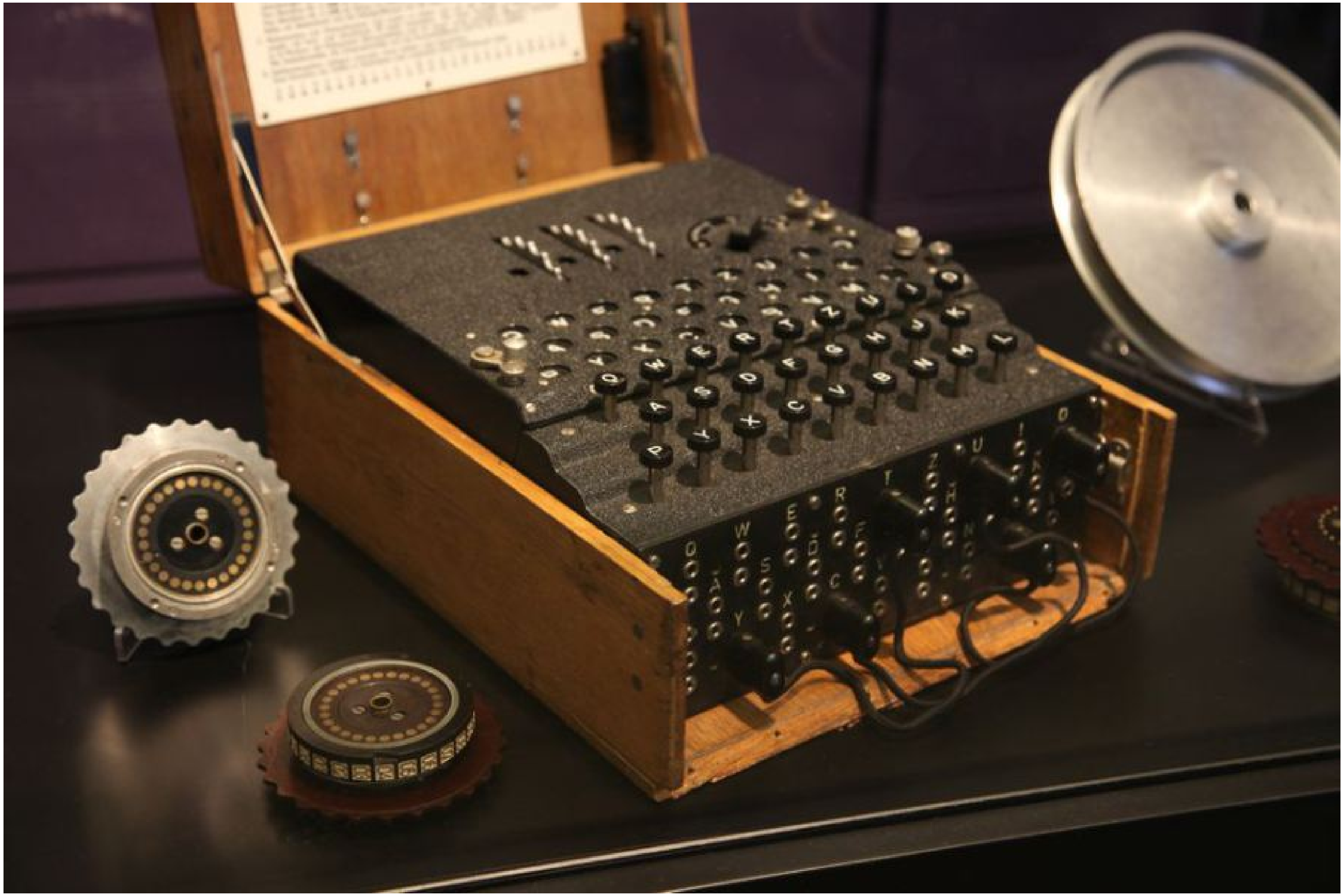
One-Time Pad

- Truly random
- Used only once
- Maximum entropy

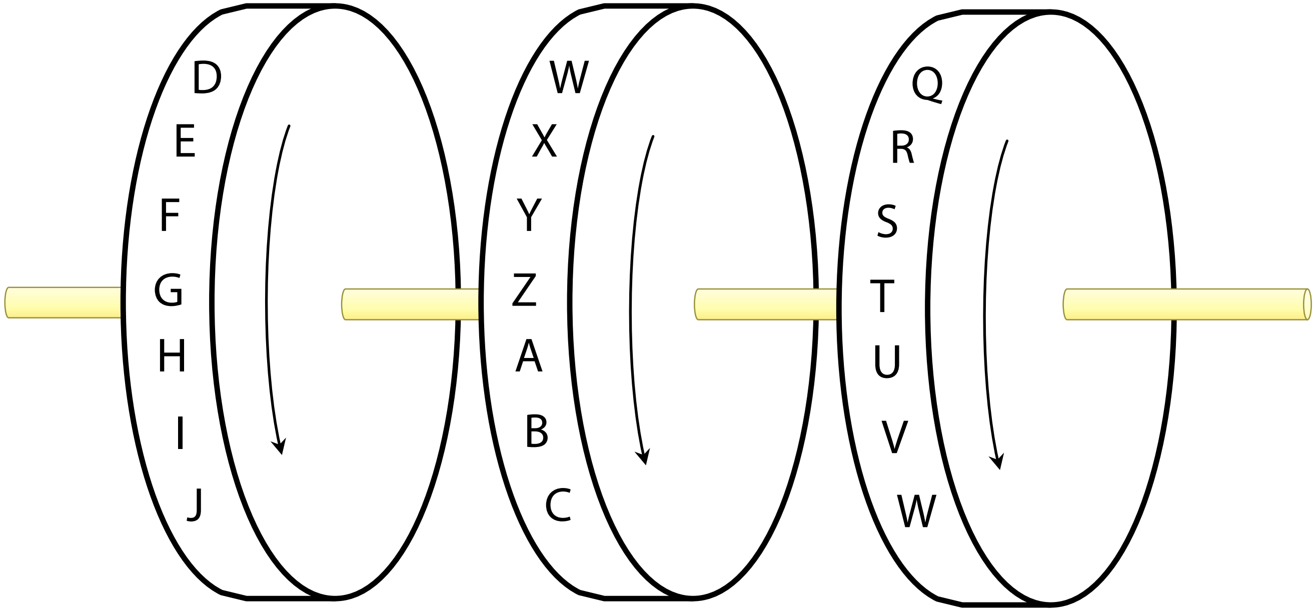
- Mistakes are common
- Hard to use
- Compromised

The Enigma Machine

The Enigma Machine

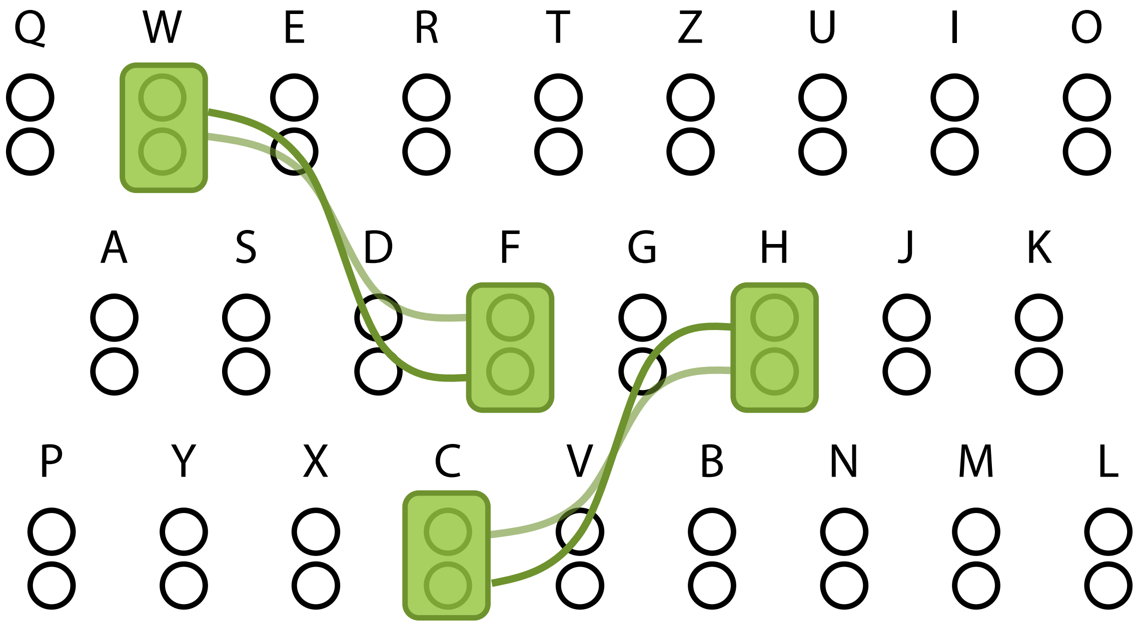


Advancing Rotors



2x

Plug Board



Plug Board

$$\frac{\overbrace{26 \text{ x } 25 \text{ x } 24 \text{ x } 23 \text{ x } 22 \text{ x } 21 \text{ x } 20 \text{ x } 19 \text{ x } 18 \text{ x } 17 \text{ x } 16 \text{ x } 15}^{\text{Select 12 letters}}}{\underbrace{6 \text{ x } 5 \text{ x } 4 \text{ x } 3 \text{ x } 2 \text{ x } 1}_{\text{Select 6 cables}} \quad \text{x} \quad \underbrace{2 \text{ x } 2 \text{ x } 2 \text{ x } 2 \text{ x } 2 \text{ x } 2}_{\text{Reverse 6 cables}}}$$

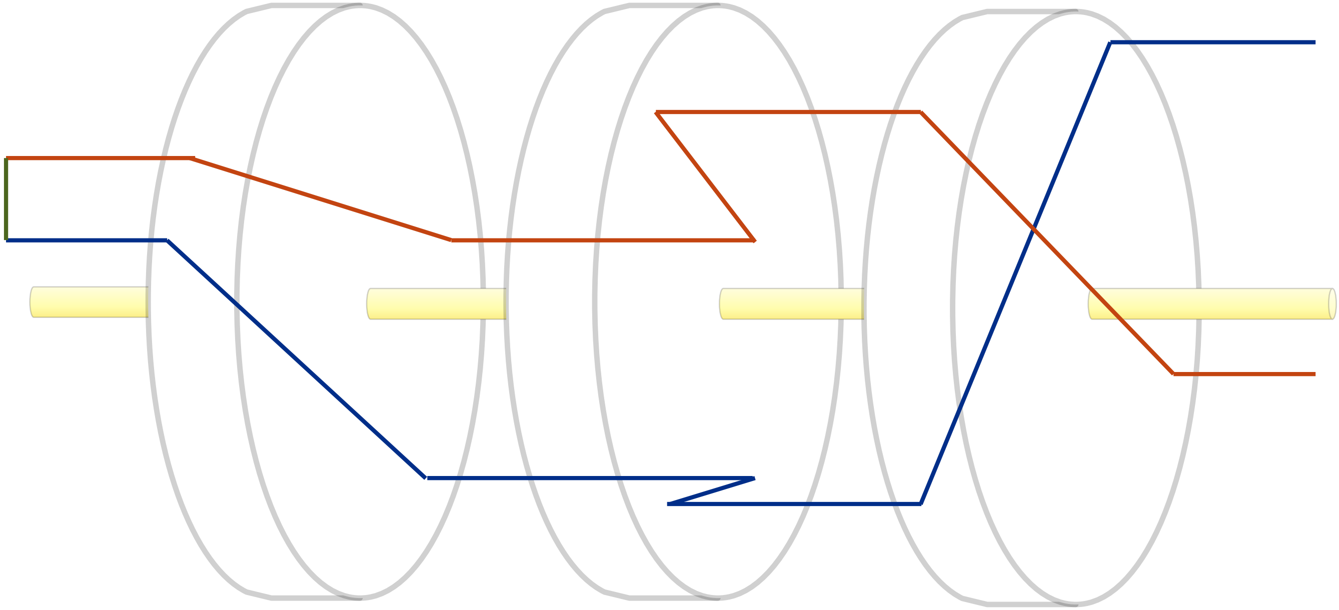
$$= 100{,}391{,}791{,}500$$

Plug Board

$$\frac{\overbrace{26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19 \times 18 \times 17 \times 16 \times 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8 \times 7}^{\text{Select 20 letters}}}{\underbrace{10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}_{\text{Select 10 cables}} \quad \times \quad \underbrace{2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2}_{\text{Reverse 10 cables}}}$$

$$= 150{,}738{,}274{,}937{,}250$$

Decryption



Rotor Pattern

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

Entropy

of a 26-letter sequence

One-Time Pad: 4.7 x 26 = 122.2

Enigma Rotor: 4.7

Entropy

of one output letter

Without Reflector: $\log_2(26) = 4.7$

With Reflector: $\log_2(25) = 4.6$

Rotor Combinations

Single Stepping: 26 x 26 x 26 = 17,576

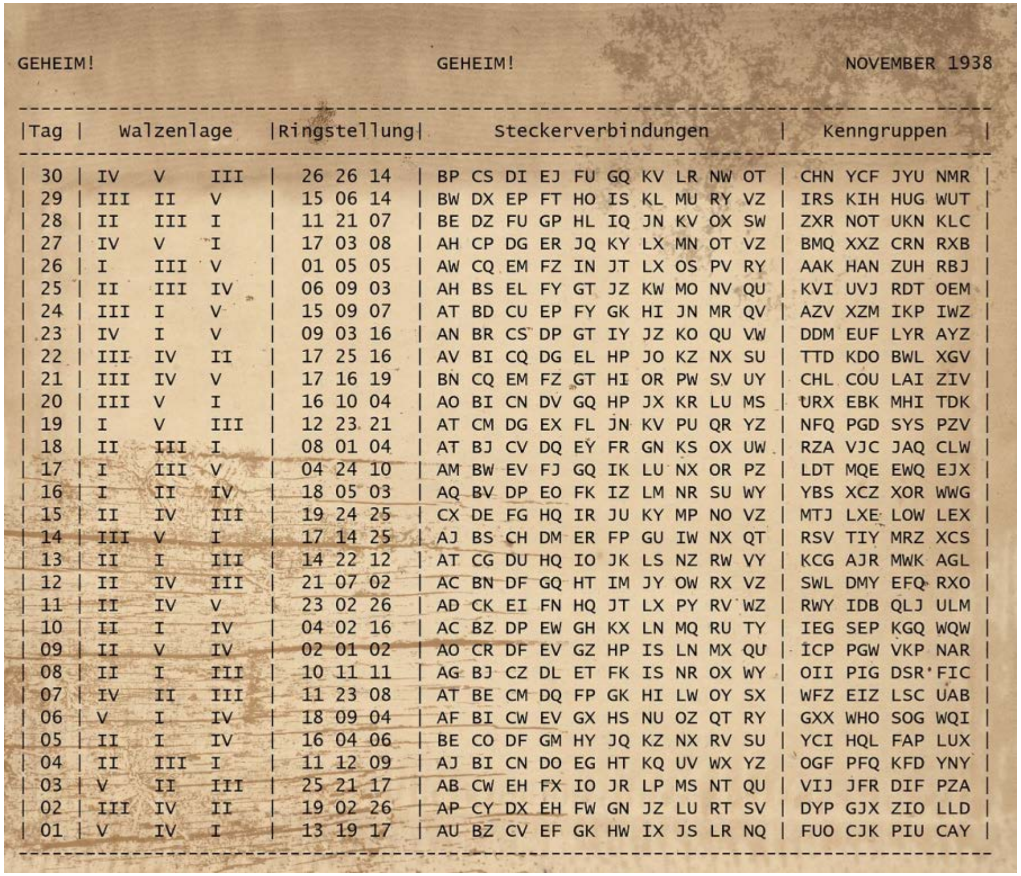
Double Stepping: 26 x 25 x 26 = 16,900

Procedure Mistakes

- Same initial rotor settings for a day
- No repeated initial rotor settings in a month
- Encrypt key twice in a message
- Send same message encrypted differently

Biggest Mistake

- Daily plug board configurations
- $\log_2(150{,}738{,}274{,}937{,}250) = 47.1$ bits!



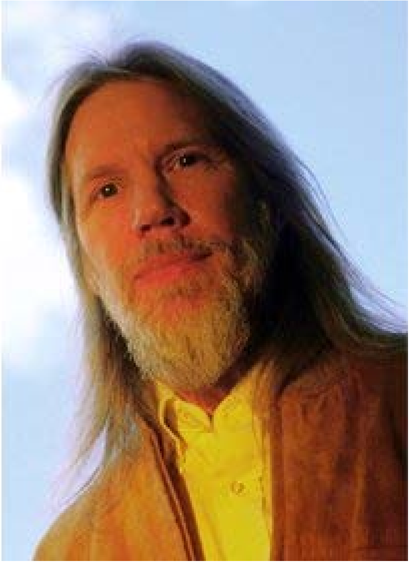
GEHEIM! GEHEIM! NOVEMBER 1938

Tag	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppen
30	IV V III	26 26 14	BP CS DI EJ FU GQ KV LR NW OT	CHN YCF JYU NMR
29	III II V	15 06 14	BW DX EP FT HO IS KL MU RY VZ	IRS KIH HUG WUT
28	II III I	11 21 07	BE DZ FU GP HL IQ JN KV OX SW	ZXR NOT UKN KLC
27	IV V I	17 03 08	AH CP DG ER JQ KY LX MN OT VZ	BMQ XXZ CRN RXB
26	I III V	01 05 05	AW CQ EM FZ IN JT LX OS PV RY	AAK HAN ZUH RBJ
25	II III IV	06 09 03	AH BS EL FY GT JZ KW MO NV QU	KVI UVJ RDT OEM
24	III I V	15 09 07	AT BD CU EP FY GK HI JN MR QV	AZV XZM IKP IWZ
23	IV I V	09 03 16	AN BR CS DP GT IY JZ KO QU VW	DDM EUF LYR AYZ
22	III IV II	17 25 16	AV BI CQ DG EL HP JO KZ NX SU	TTD KDO BWL XGV
21	III IV V	17 16 19	BN CQ EM FZ GT HI OR PW SV UY	CHL COU LAI ZIV
20	III V I	16 10 04	AO BI CN DV GQ HP JX KR LU MS	URX EBK MHI TDK
19	I V III	12 23 21	AT CM DG EX FL JN KV PU QR YZ	NFQ PGD SYS PZV
18	II III I	08 01 04	AT BJ CV DQ EY FR GN KS OX UW	RZA VJC JAQ CLW
17	I III V	04 24 10	AM BW EV FJ GQ IK LU NX OR PZ	LDT MQE EWQ EJX
16	I II IV	18 05 03	AQ BV DP EO FK IZ LM NR SU WY	YBS XCZ XOR WWG
15	II IV III	19 24 25	CX DE FG HQ IR JU KY MP NO VZ	MTJ LXE LOW LEX
14	III V I	17 14 25	AJ BS CH DM ER FP GU IW NX QT	RSV TIY MRZ XCS
13	II I III	14 22 12	AT CG DU HQ IO JK LS NZ RW VY	KCG AJR MWK AGL
12	II IV III	21 07 02	AC BN DF GQ HT IM JY OW RX VZ	SWL DMY EFQ RXO
11	II IV V	23 02 26	AD CK EI FN HQ JT LX PY RV WZ	RWY IDB QLJ ULM
10	II I IV	04 02 16	AC BZ DP EW GH KX LN MQ RU TY	IEG SEP KGQ WQW
09	II V IV	02 01 02	AO CR DF EV GZ HP IS LN MX QU	ICP PGW VKP NAR
08	II I III	10 11 11	AG BJ CZ DL ET FK IS NR OX WY	OII PIG DSR FIC
07	IV II III	11 23 08	AT BE CM DQ FP GK HI LW OY SX	WFZ EIZ LSC UAB
06	V I IV	18 09 04	AF BI CW EV GX HS NU OZ QT RY	GXX WHO SOG WQI
05	II I IV	16 04 06	BE CO DF GM HY JQ KZ NX RV SU	YCI HQL FAP LUX
04	II III I	11 12 09	AJ BI CN DO EG HT KQ UV WX YZ	OGF PFQ KFD YNY
03	V II III	25 21 17	AB CW EH FX IO JR LP MS NT QU	VIJ JFR DIF PZA
02	III IV II	19 02 26	AP CY DX EH FW GN JZ LU RT SV	DYP GJX ZIO LLD
01	V IV I	13 19 17	AU BZ CV EF GK HW IX JS LR NQ	FUO CJK PIU CAY

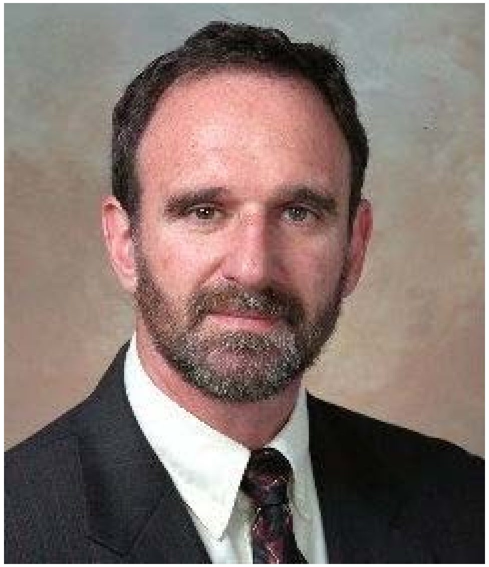
More Frequent Configurations

- **Fewer intercepts**
  - Harder to crack
- **More time per message**
  - One day: military advantage
  - One week: history lesson
- **Protect the most significant improvement**

Diffie-Hellman



Whitfield Diffie



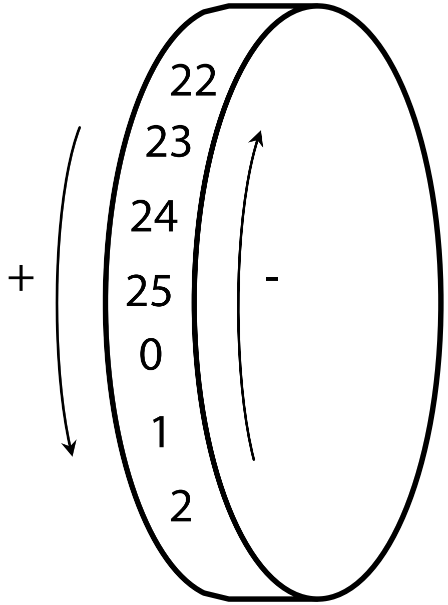
Martin Hellman

Ralph Merkle

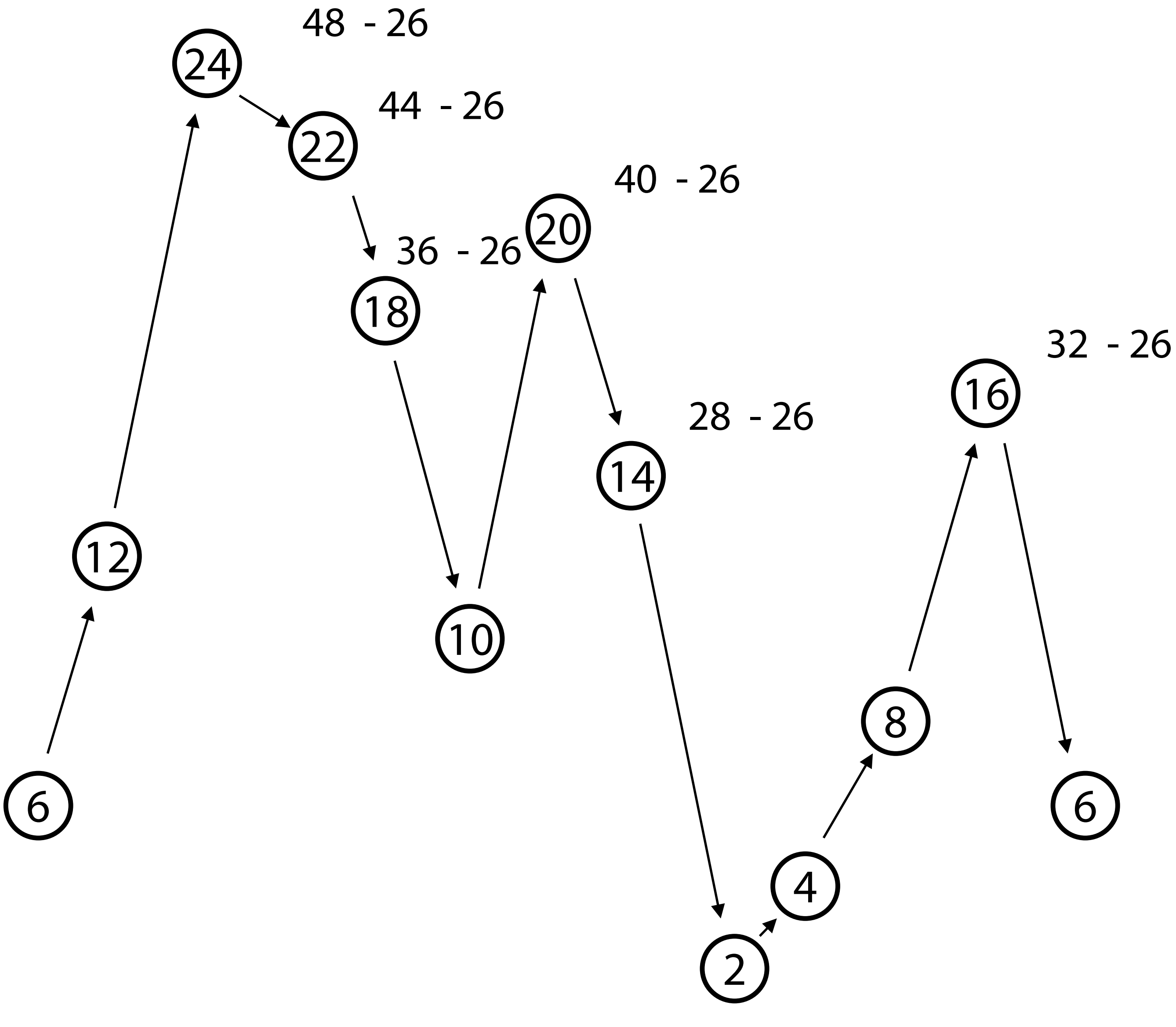
Shared Secret

Untrusted Channel

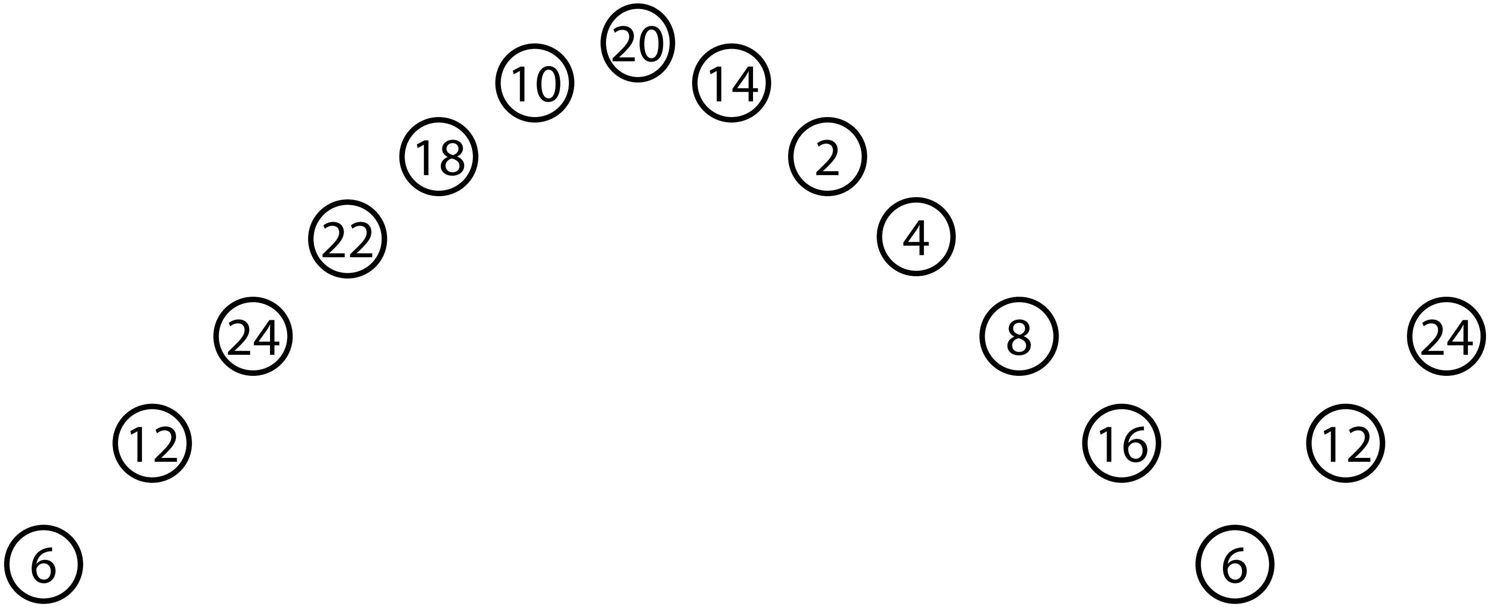
Modulo Addition and Subtraction



Modulo Multiplication

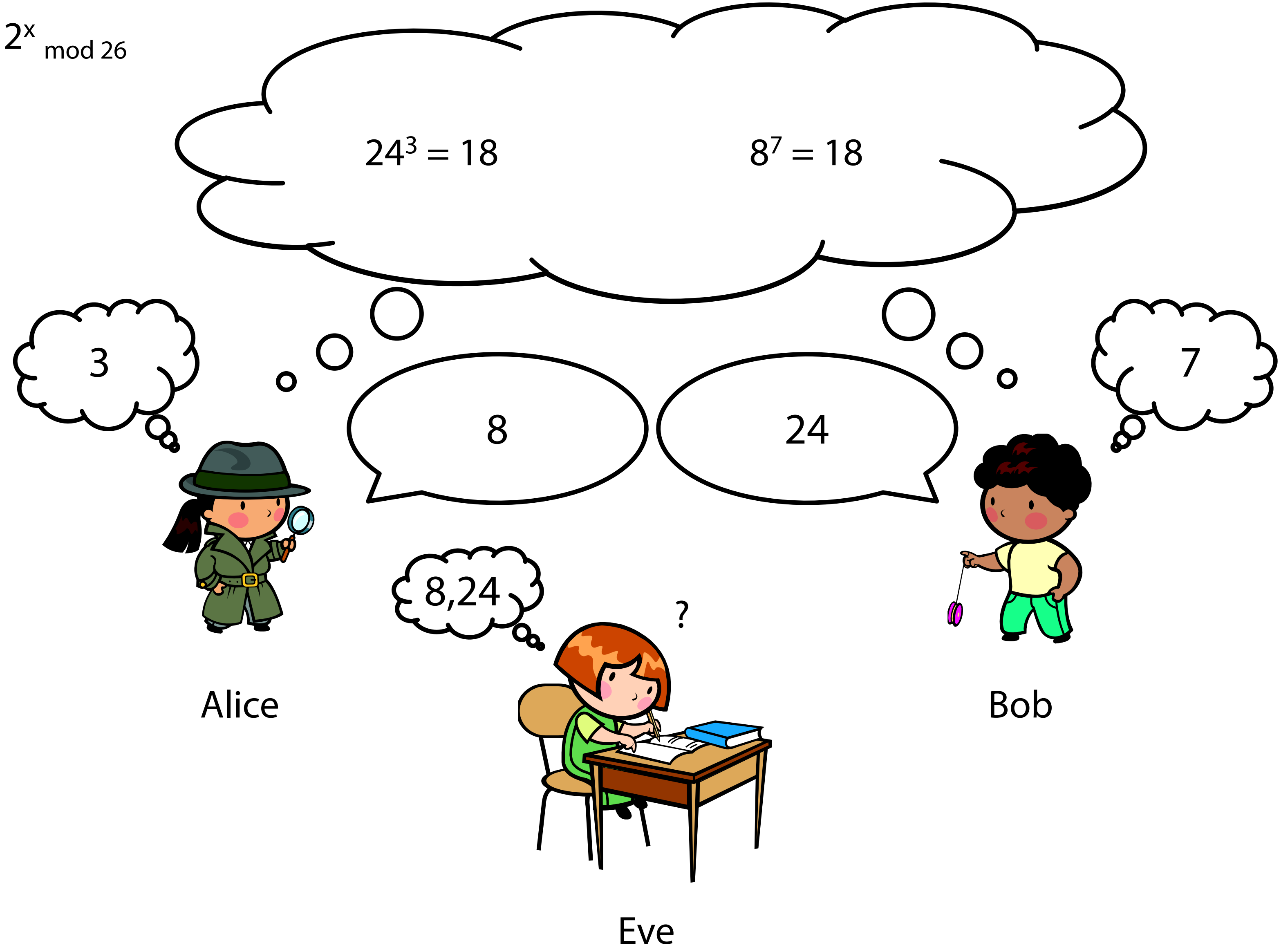


Modulo Multiplication



Secret Communications

2^x mod 26



Algebra Refresher

$$ab = ba$$

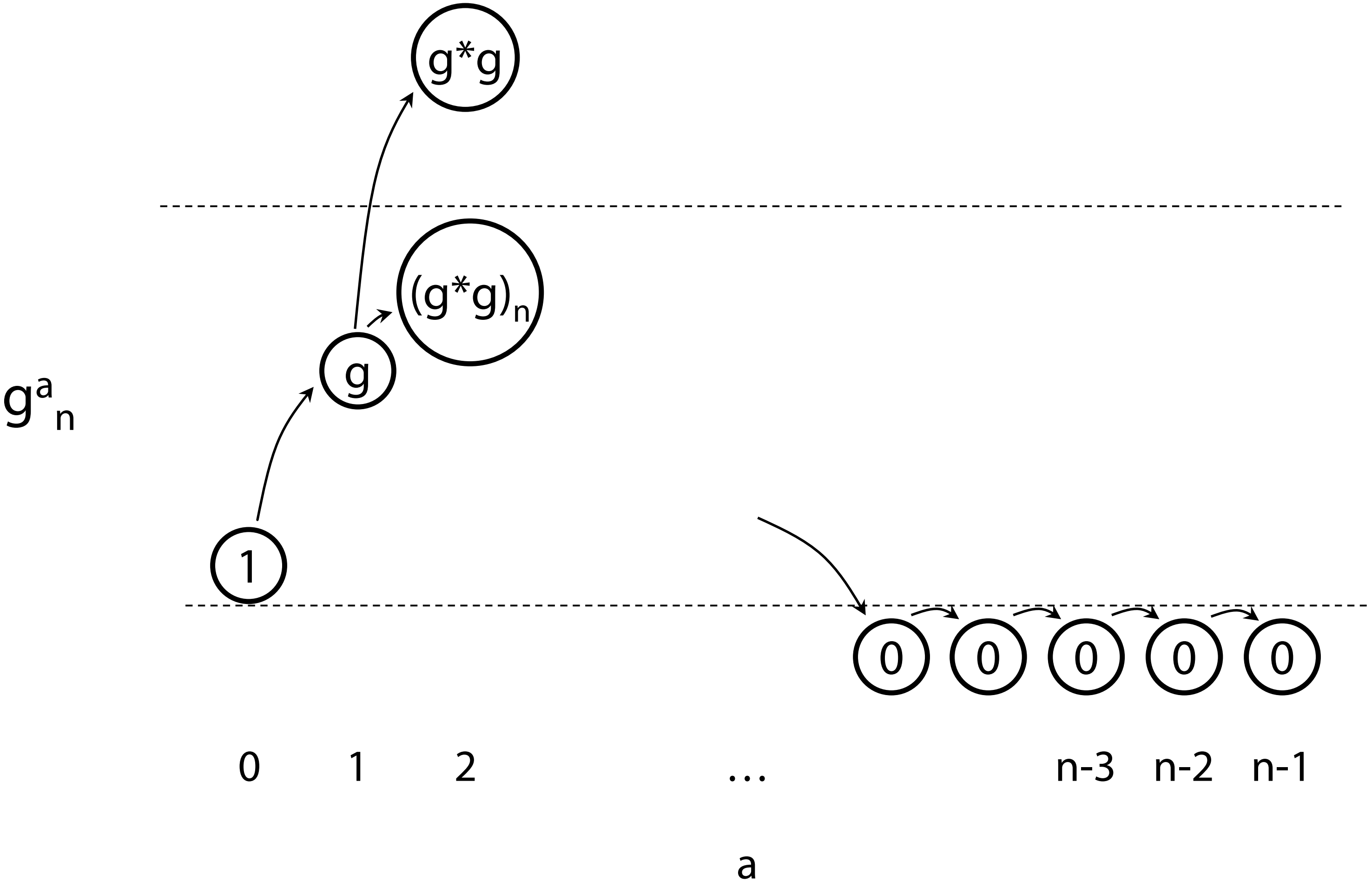
$$(g^a)^b = g^{ab}$$

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

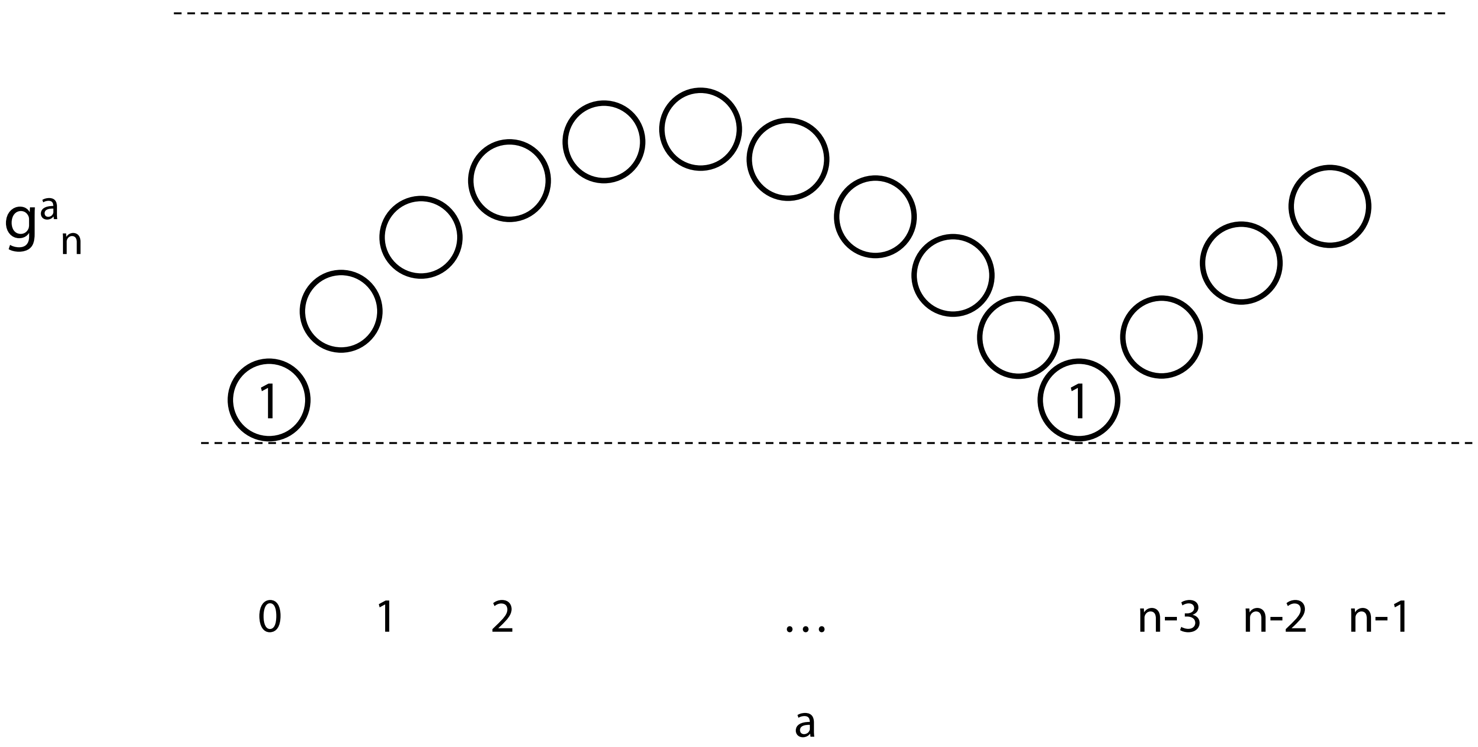
$$(g^a)^b = (g^b)^a$$

$$(g^a{}_{\text{mod } n})^b{}_{\text{mod } n} = (g^b{}_{\text{mod } n})^a{}_{\text{mod } n}$$

Exponentiation in a Modulus

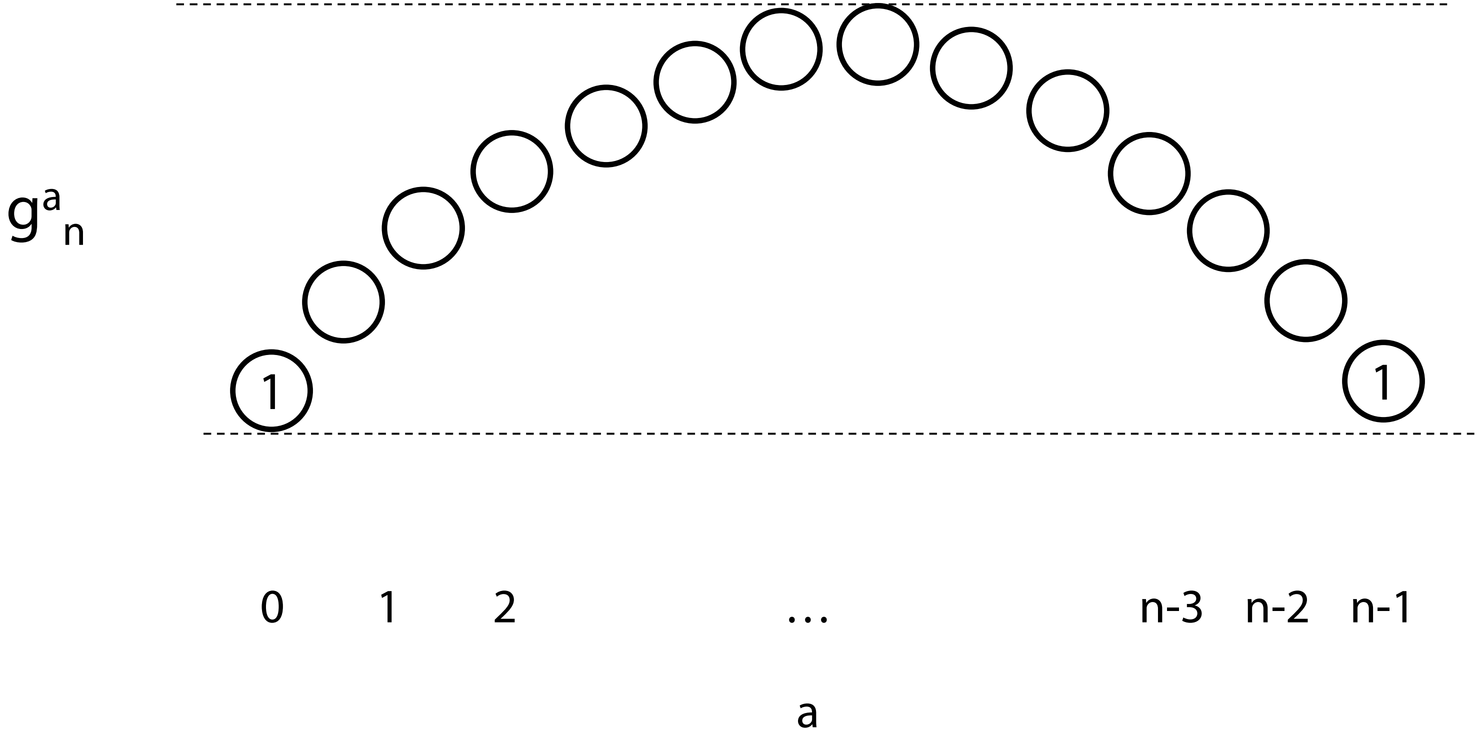


Exponentiation in a Modulus



Exponentiation in a Modulus

$$g^{n-1} \bmod n = 1$$



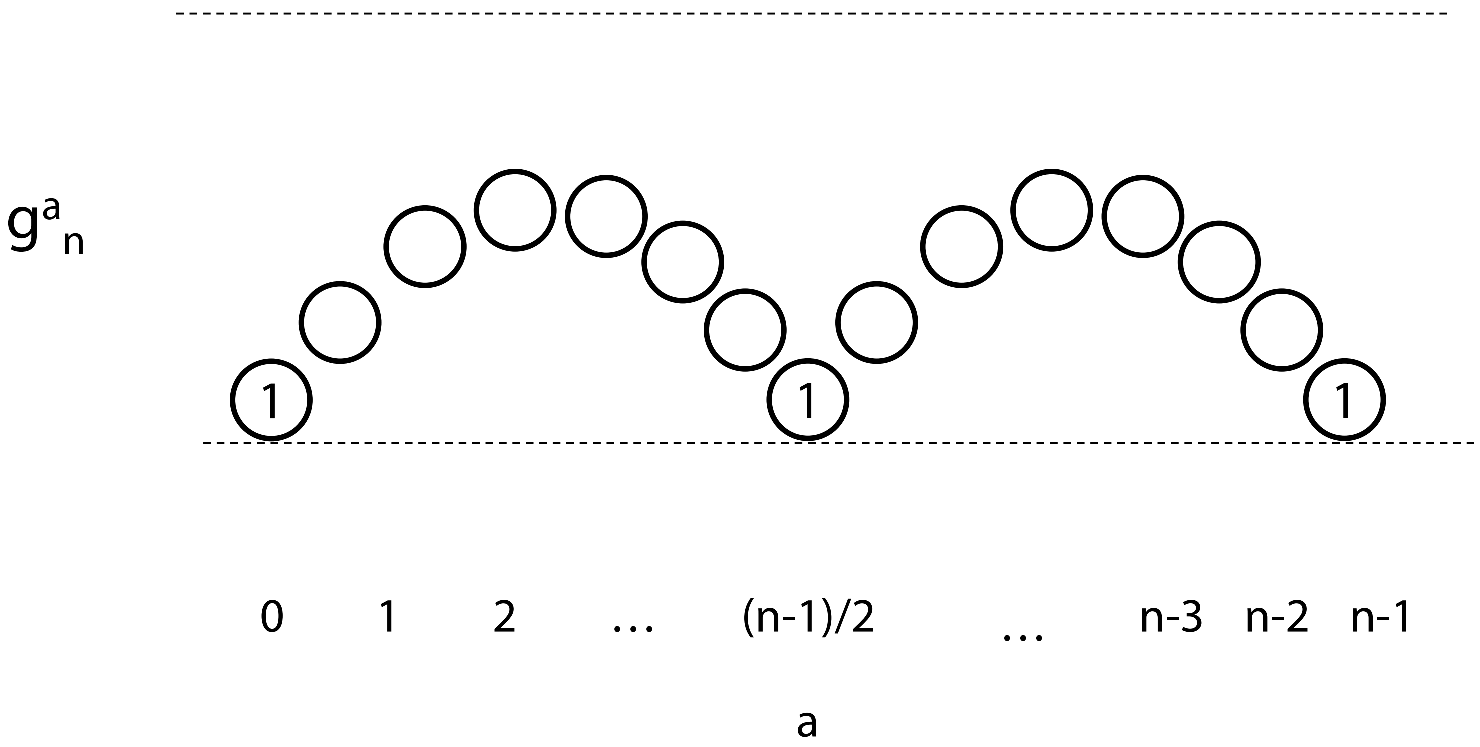
Fermat’s Little Theorem

$$g^{n-1} \bmod n = 1$$

if n is prime

and g is not a multiple of n

Premature Cycles



Large Primes

2048 bits

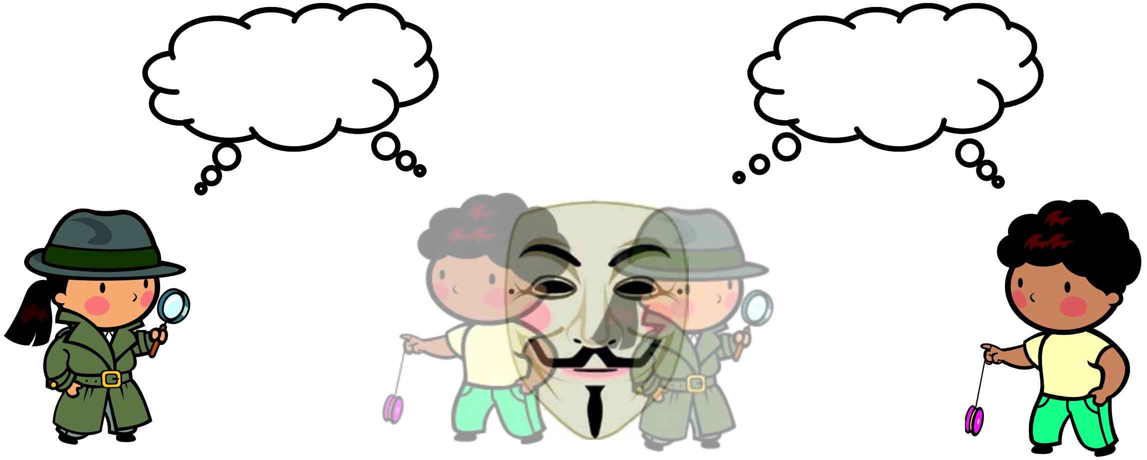
616 digits

10,000,000,000,000,000,000,000,000,000,000,000,000, … ,000,000,000,000,000,000,000,000,000,000,000,000,000

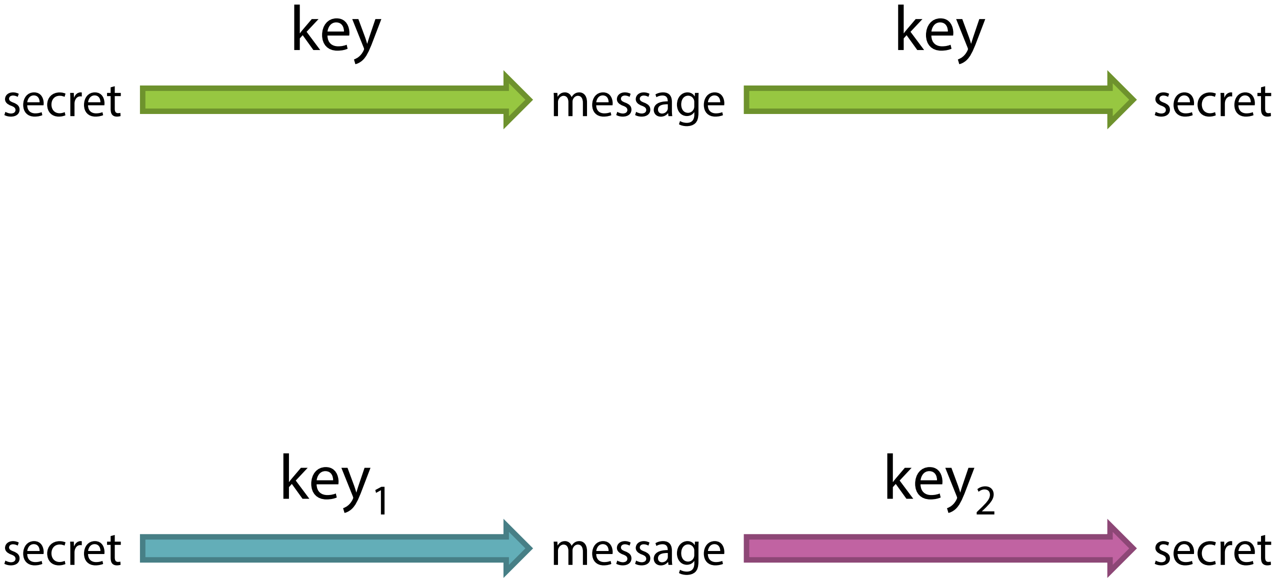
46 digits

10, 000,000, … ,000,000

Man in the Middle



Asymetric Cryptography



key key

secret message secret

key$_1$ key$_2$

secret message secret

Rest of the Course

- Modern cryptographic methods
- Mathematics
- Flaws
- Mistakes

Conclusion

- Entropy
- One-time pad
- Patterns can be exploited
- Weakest link: human operator