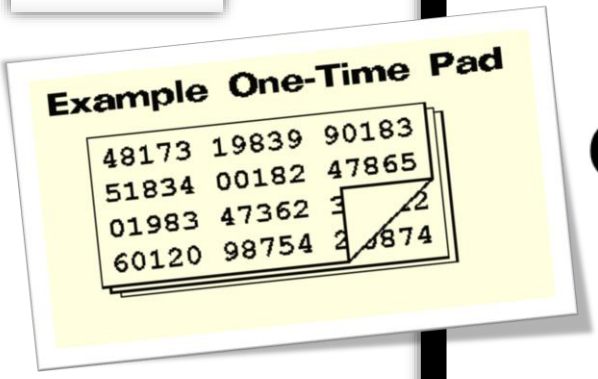
One-Time Pad



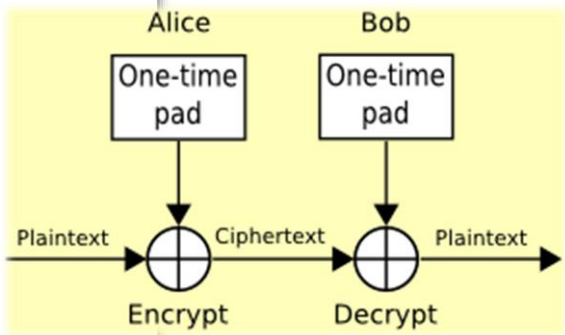
One-Time Pad

Dr. Bashar M. Nema
Mustansiriyah University

A stream encryption is the encryption of each letter one by one,

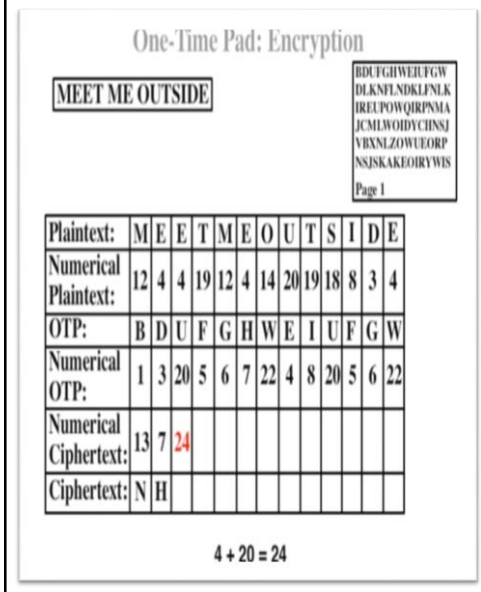
One-Time Pad: Encryption

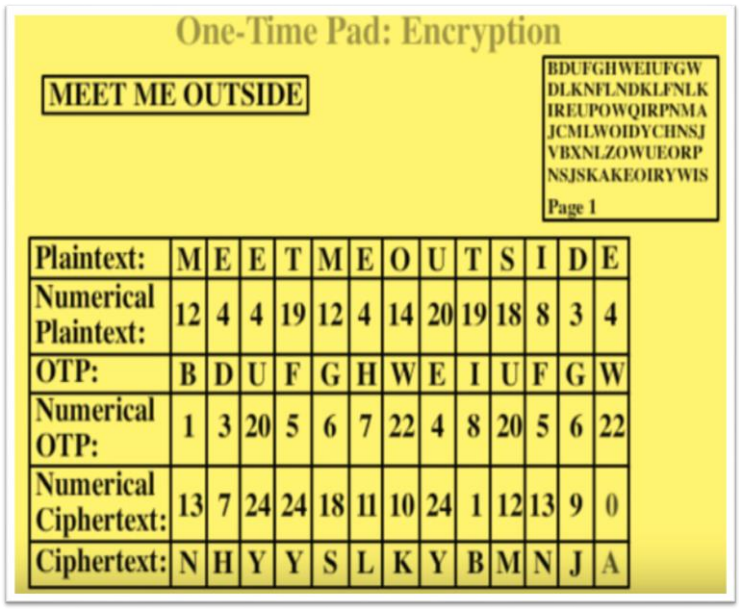
BDUFGHWEIUFGW DLKNFLNDKLFNLK IREUPOWQIRPNMA JCMLWOIDYCHNSJ VBXNLZOWUEORP NSJSKAKEOIRYWIS Page 1	PNDHFUWERMCAM JKSQZXLSODWBWI SNALAPQOERCIROT MHSOWLBTPYIAVX JALAKENBTOWQPM ZXZMSHWEORPTPS Page 2
HJGAEWLLCHCBCI EWKLNCYTUAPLX QZMUBTCENPCYK ADLJOUNVXRSGNK SYHCRNIQTCONFU JGVEWSHOPMKCY Page 3	CCHXRETWAAAHJ AWRCIOHSRYPIV WAEOIHFGRTLCG LPLIIVHHCXXCSH ZYIEWNMKPRGH BDRTYUIOMNSNU Page 4

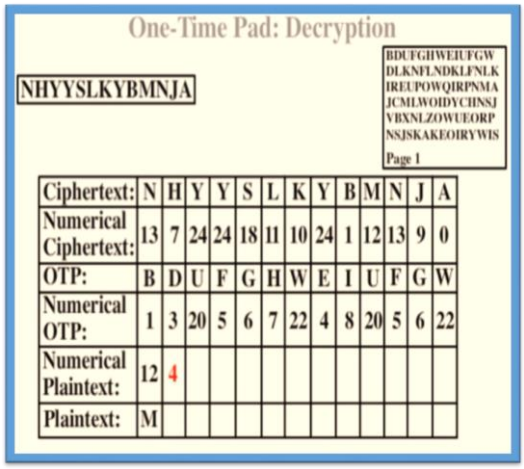


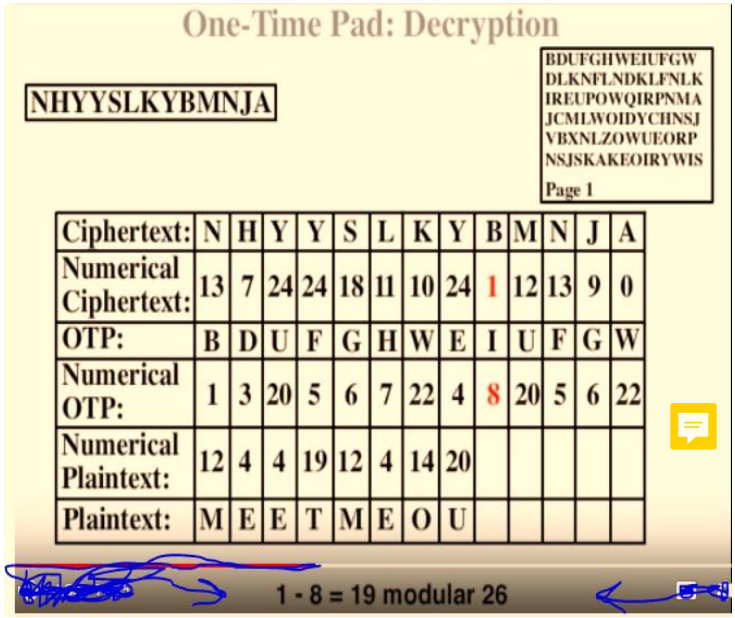
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Alice and Bob each have a copy of the same One Time Pad


One-Time Pad: Encryption
MEET ME OUTSIDE
BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS
Page 1
Plaintext: M E E T M E O U T S I D E
Numerical Plaintext: 12 4 4 19 12 4 14 20 19 18 8 3 4
OTP: B D U F G H W E I U F G W
Numerical OTP: 1 3 20 5 6 7 22 4 8 20 5 6 22
Numerical Ciphertext: 13 7 24
Ciphertext: N H
4 + 20 = 24


One-Time Pad: Encryption
MEET ME OUTSIDE
BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS
Page 1
Plaintext: M E E T M E O U T S I D E
Numerical Plaintext: 12 4 4 19 12 4 14 20 19 18 8 3 4
OTP: B D U F G H W E I U F G W
Numerical OTP: 1 3 20 5 6 7 22 4 8 20 5 6 22
Numerical Ciphertext: 13 7 24 24 18 11 10 24 1 12 13 9 0
Ciphertext: N H Y Y S L K Y B M N J A


One-Time Pad: Decryption
NHYYSLKYBMNJA
BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS
Page 1
Ciphertext: N H Y Y S L K Y B M N J A
Numerical Ciphertext: 13 7 24 24 18 11 10 24 1 12 13 9 0
OTP: B D U F G H W E I U F G W
Numerical OTP: 1 3 20 5 6 7 22 4 8 20 5 6 22
Numerical Plaintext: 12 4
Plaintext: M


One-Time Pad: Decryption
NHYYSLKYBMNJA
BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS
Page 1
Ciphertext: N H Y Y S L K Y B M N J A
Numerical Ciphertext: 13 7 24 24 18 11 10 24 1 12 13 9 0
OTP: B D U F G H W E I U F G W
Numerical OTP: 1 3 20 5 6 7 22 4 8 20 5 6 22
Numerical Plaintext: 12 4 4 19 12 4 14 20
Plaintext: M E E T M E O U
1 - 8 = 19 modular 26

One-Time Pad: Decryption

NHYYSLKYBMNJA

BDUFGHWEIUFGW
DLKNFLNDKLFNLK
IREUPOWQIRPNMA
JCMLWOIDYCHNSJ
VBXNLZOWUEORP
NSJSKAKEOIRYWIS

Page 1

Ciphertext:	N	H	Y	Y	S	L	K	Y	B	M	N	J	A
Numerical Ciphertext:	13	7	24	24	18	11	10	24	1	12	13	9	0
OTP:	B	D	U	F	G	H	W	E	I	U	F	G	W
Numerical OTP:	1	3	20	5	6	7	22	4	8	20	5	6	22
Numerical Plaintext:	12	4	4	19	12	4	14	20	19	18	8	3	4
Plaintext:	M	E	E	T	M	E	O	U	T	S	I	D	E