The History of Cryptography

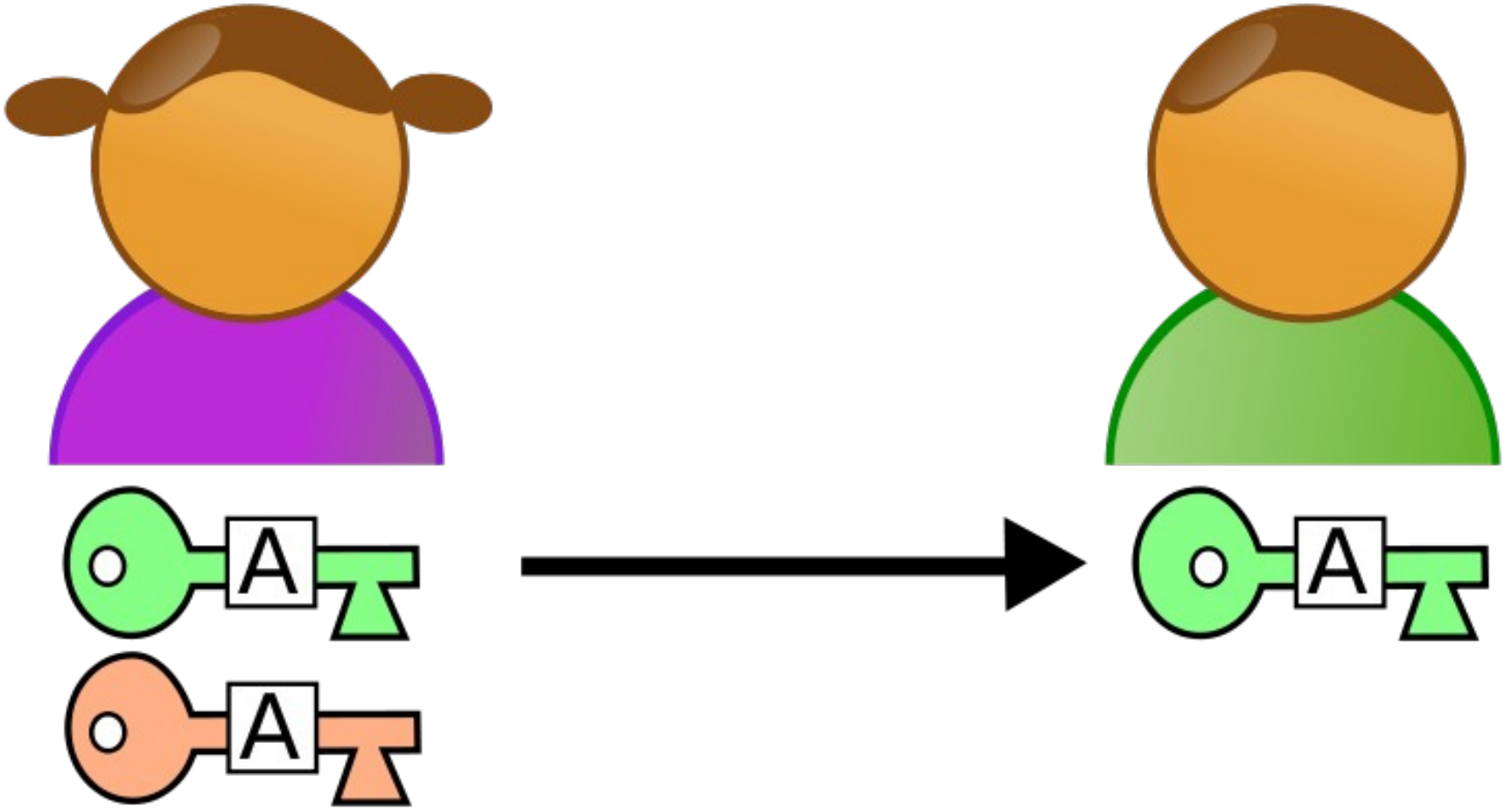
Portland Underground Grad School

Erik L. Arneson
http://arnesonium.com/crypto

Principle Concepts

- Predictability and Randomness
- Security and Usability
- Identity and Trust
- Thinking Like an Attacker

Alice and Bob



Chuck and Eve

Atbash Cipher

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

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

HELLO MOTHER

SVOOL NLGSVI

Caesar Cipher

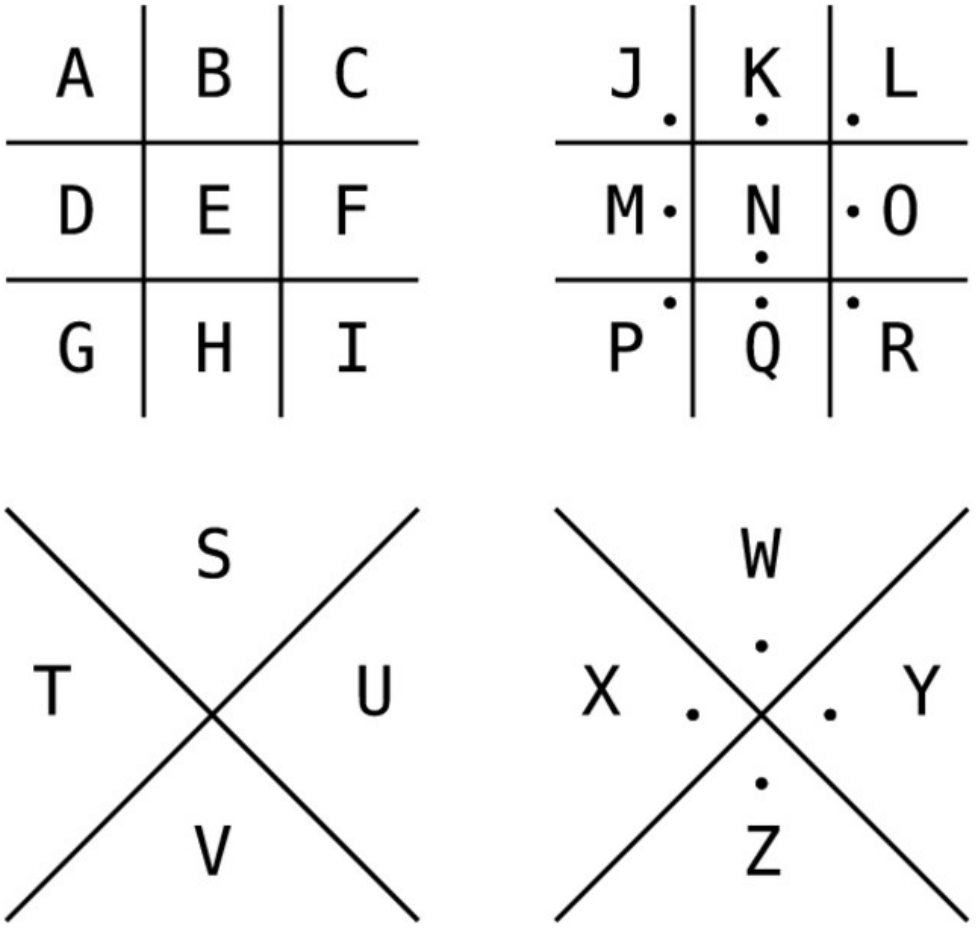
A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

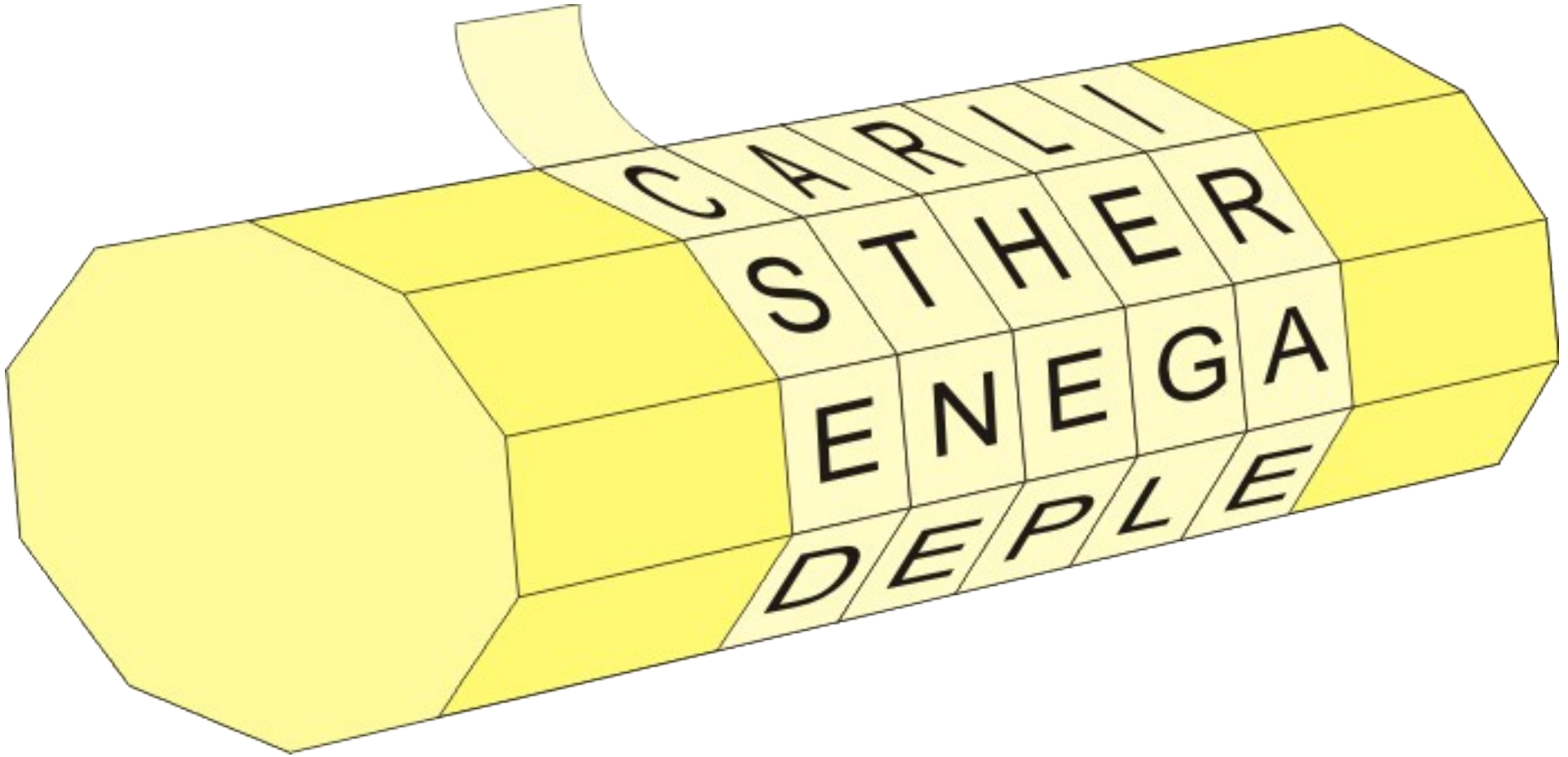
HELLO MOTHER

KHOOR PRWKHU

Pigpen Cipher



Scytale



Route Cipher

C	R	Y	P	T
O	G	R	A	P
H	Y	I	S	R
E	A	L	L	Y
G	R	E	A	T

COHEG RGYAR YRILE PASLA TPRYT

TYRPT PYRCO HEGRE ALSAR GYALI

Columnar Cipher

P	I	N	T	S
D	E	F	E	N
D	T	H	E	W
A	L	L	S	O
F	T	H	E	C
A	S	T	L	E

I	N	P	S	T
E	F	D	N	E
T	H	D	W	E
L	L	A	O	S
T	H	F	C	E
S	T	A	E	L

ETLTS FHLHT DDAFA NWOCE EESEL

Homework: Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M
T	H	E	Q	U	I	C	K	B	R	O	W	N

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	X	J	U	M	P	D	V	L	A	Z	Y	G