CSCM 18 CRYPTOGRAPHY AND IT SECURITY
COURSEWORK 1

TSEPO NYAKONDA
2009489

2 NOVEMBER 2021

Part 1.
Question1;
Weak links in smart homes_:

Humans: if humans are ignorant, they're prone to disregarding security protocols, leaving systems vulnerable

Network: network misconfiguration may result in vulnerabilities within the system

SmartHome Devices: They're prone to attacks if they're connected to the internet

Communication between devices: a vector for eavesdropping / man in the middle attacks

Question 2:

Symmetric key cryptography relies on a shared key between two parties. Asymmetric key cryptography uses a public-private key pair where one key is used to encrypt and the other to decrypt.

Part 2: Transposition Cipher
Question 3:
ALAN TURING THE ENIGMA MACHINE in rail 2 cipher;

A		A		T		R		N		T		E		N		G		A		A		H		N		
	L		N		U		I		G		H		E		I		M		M		C		I		E	

CipherText: AATRNTENGAAHNLNUIGHEIMMCIE

ALAN TURING THE ENIGMA MACHINE in rail 3 cipher;

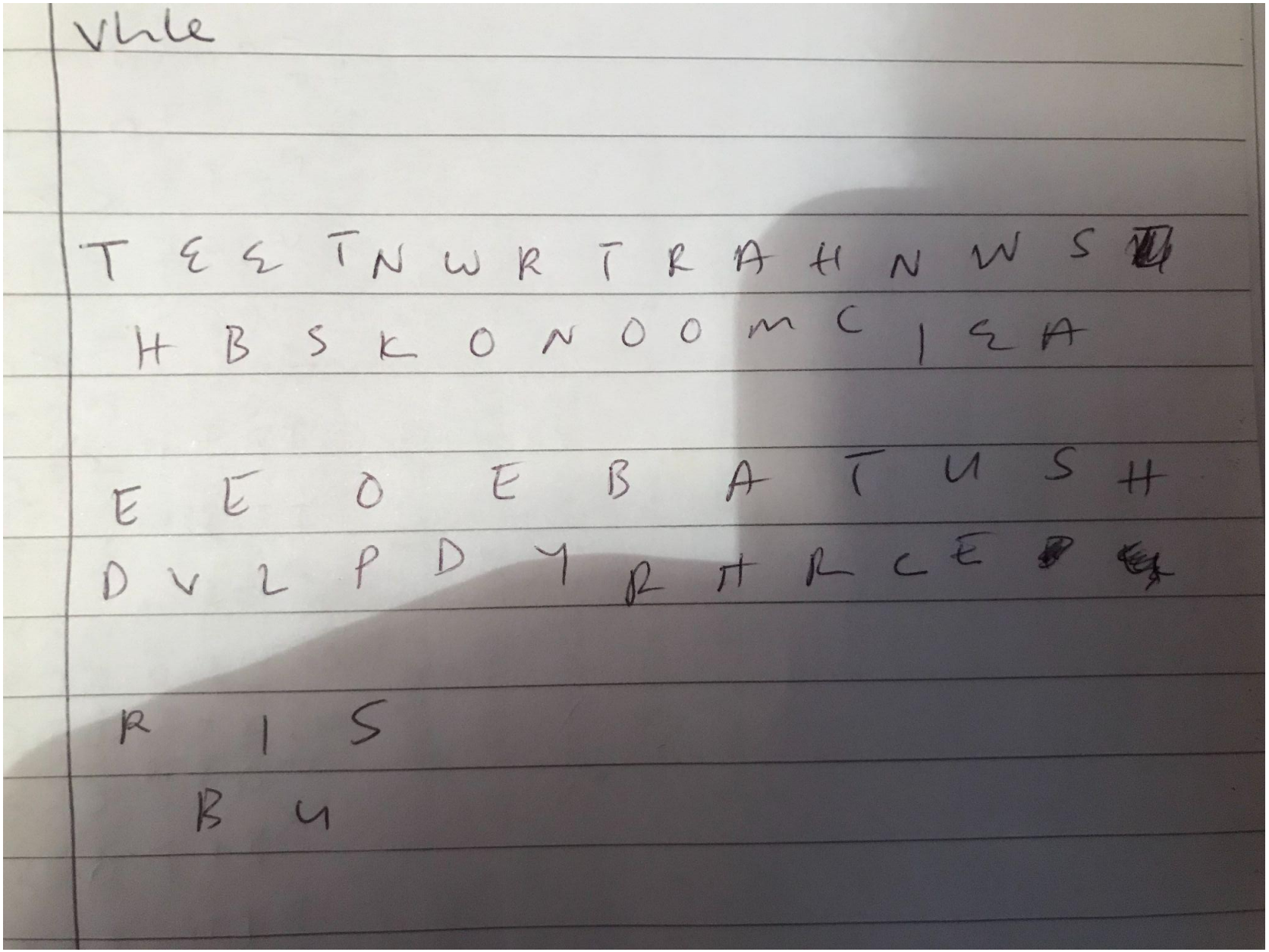
A				T				N				E				G				A				N		
	L		N		U		I		G		H		E		I		M		M		C		I		E	

		A				R				T				N				A				H				

CipherText: ATNEGANLNUIGHEIMMCIEARTNAH

Question 4;

Decipher TEETNWRTRAHNWSEEOEBATUSHRISHBSKONOOMCIEADVLPDYRHRCEBU in rail 2;


while

Text us : thebestknownrotormachinewasdevelopedbyarthurscherbius
Question 5:
Encipher THE JOKER SAID IT WAS ALL PART OF THE PLAN, using column 5,
KEY: MyUni

M	Y	U	N	I
2	5	4	3	1
T	H	E	J	O
K	E	R	S	A
I	D	T	H	A
T	I	T	W	A
S	A	L	L	P
A	R	T	O	F
T	H	E	P	L
A	N			

CipherText: OAAAPFLTKITSATAJSHWLOPERTTLTEHEDIARHN

Part 3: Shift and Polyalphabetic Ciphers

Question 6; “Encrypt Cryptography is cool” using shift 6-

C	R	Y	P	T	O	G	R	A	P	H	Y		I	S		C	O	O	L
I	X	E	V	Z	U	M	X	G	V	N	E		O	Y		I	U	U	R

Question 7:

Question 8:

Monoalphabetic cipher utilizes a mixed alphabet and replaces a letter of the normal alphabet with it.

Polyalphabetic cipher is based on substitution, using multiple substitution alphabets. The alphabet is always substituted by a different random alphabet. This makes it much more complicated to decode.