Revision Notes Cryptography April 1st 2019

Question 1

Define perfect secrecy for the following two cases: (1) when one of characters of the plaintext is known to an attacker and (2) when one of the characters of the ciphertext is known to an attacker. Prove that the definition in case 1 is correct if and only if the definition in case 2 is correct.

Lemma: OTP has perfect secrecy.

Proof:

$$\forall m, c : Pr\left[E(k,m) = c\right] = \frac{\#keys\ k \in \mathcal{K}\ s.t.\ E(k,m) = c}{|\mathcal{K}|}$$

So: if $\forall m, c : \#\{k \in \mathcal{K} : E(k,m) = c\} = const$

= Cipher has perfect Secrecy

Solution: Let M be the set of all possible plaintext characters and C be the set of all possible ciphertext characters.
In case 1, one of the characters of the plaintext (let m be the character) is known to the attacker. In perfect secrecy, knowing one of characters should not reveal anything about the rest of the ciphertext. Therefore, the definition (def1) in this case will be:

Pr [C=c| M=m] = Pr [C=c] where c∈C

***(a* ∈ *S* means *a* is an element of the set *S*; *a* ∉ *S* means *a* is not an element of *S*.)**

In Case 2, one of the characters of the ciphertext (let c be the character) is known to the attacker. In perfect secrecy, knowing one of the characters of ciphertexts should not reveal anything about next messages.

Therefore, the definition in this case (def2) will be:
Pr [M=m| C=c] = Pr [M=m] where M∈m

Now watch this:

https://www.khanacademy.org/partner-content/wi-phi/wiphi-critical-thinking/wiphi-fundamentals/v/bayes-theorem

Probability Formulas

- The following is one of the most crucial theorems in probability:

Bayes' Theorem

If $p(Y = y) > 0$

then $p(X = x|Y = y) = \frac{p(X = x, Y = y)}{p(Y = y)}$

$= \frac{p(Y = y|X = x) \times p(X = x)}{p(Y = y)}$

- X and Y are independent iff p(X = x | Y = y) = p(X = x)
  - i.e. value of X does not depend on the value of Y .
- Law of total probability

$$P(B) = \sum_j P(B \mid A_j) P(A_j),$$

Prove def1 => def2

Def1=>Pr[C=c| M=m] = Pr(M=m| C=c) * Pr(C =c) / Pr(M=m) => Bayes theorem Eq. 1
Putting Eq 1 in def 1
Pr(M=m| C=c) * Pr(C =c) / Pr(M=m) = Pr(C=c)
=>Pr [M=m| C=c] = Pr [M=m] => Def2

Prove def2 => def1

Def1=> Pr [M=m| C=c] = Pr(C=c| M=m) * Pr(M=m) / Pr(C=c) => Bayes theorem Eq. 2
Putting Eq. 2 in def 2.
Pr(C=c| M=m) * Pr(M=m) / Pr(C=c) = Pr[M=m]
=> **Pr [C=c| M=m] = Pr [C=c]**

Question 2

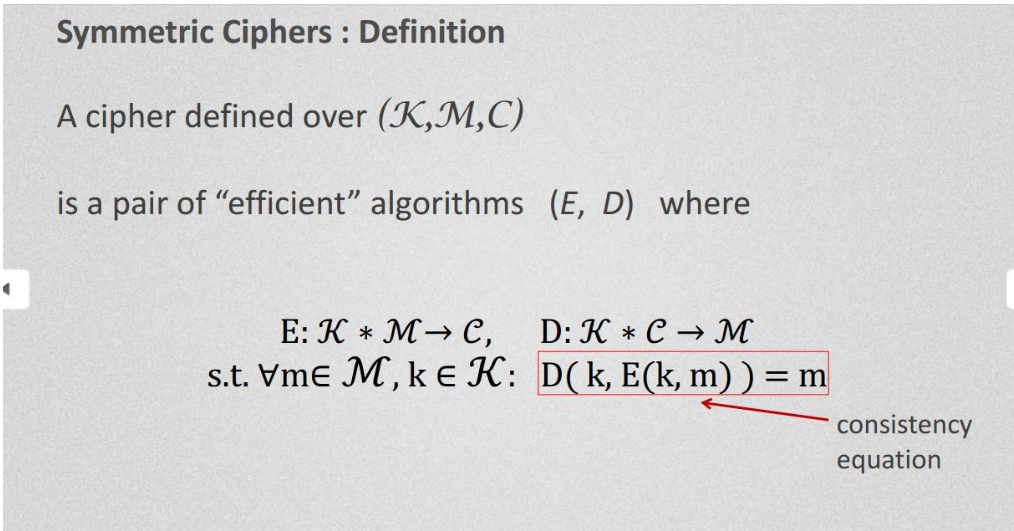
Let m be the plaintext, k be the key and ⊕ be the XOR operator. The size of plaintext (m) is equal to the size of the key (k). In encryption, the ciphertext (c) is calculated by (((m ⊕ k) ⊕ k) ⊕ k). In decryption, the plaintext (m) is calculated by (((c ⊕ k) ⊕ k) ⊕ k). Prove that the encryption and decryption schemes form a valid symmetric key cryptographic algorithm.

Solution:

Remember in Xor that the property of Self-inverse says that : A ⊕ A = 0

This means that any value XOR'd with itself gives zero.

Any value Xored with zero is unchanged.



$C := E(k, m) = k \oplus m$
$E(k, m) = k \oplus m$
$D(k, c) = k \oplus c$

$D(k,E(k, m)) = D(k,k\oplus m) = k\oplus (k\oplus m) = (k\oplus k)\oplus m = 0\oplus m = m$

Question 3

Suppose you are told that the one time pad encryption of the message "MOVE ARMY NORTH" is 6c73d5240a948c86981bc294814d6d (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one time pad encryption of the message "MOVE ARMY SOUTH" under the same OTP key

41	A	4A	J	53	S
42	B	4B	K	54	T
43	C	4C	L	55	U
44	D	4D	M	56	V
45	E	4E	N	57	W
46	F	4F	O	58	X
47	G	50	P	59	Y
48	H	51	Q	5A	Z
49	I	52	R	20	Space

	m	o	v	e	△	A	R	m	y	△	N	O	R	T	H
	4d	4F	56	45	20	41	52	4D	59	20	4E	4F	52	54	48
CT	6c	73	d5	24	0a	94	8c	86	98	16	C2	94	81	4d	6d

NORTH

4 e 4 f 5 2 5 4 4 8

0100 1110 0100 1111 0101 0010 0101 0100 0100 1000

1100 0010 1001 0100 1000 0001 0100 1101 0110 1101

C 2 9 4 8 1 4 d 6 d CT

Key 1000 1100 1101, 1011, 1101, 0011, 0001, 1001, 0010, 0101

Key 8 C D B D 3 1 9 2 5

S O U T H

53 4F 55 54 48

$$\begin{array}{r} 1000 \\ 0101 \\ \hline 1101 \end{array}$$

Binary 0101 0011 0100 1111 0101 0101 0101

5 3 4 F 5 5 5 4 4 8

0101 0011 0100 1111 0101 0101 0101 0100 0100 1000

1000 Key 1100 1101 1011 1101 0011 0001 1001, 0010, 0101

1101 1111, 1001, 0100, 1000, 0110 0100 1101 0110 1101

D (CT) F 9 4 8 6 4 D 6 D

1101

DF 94 86 4D 6D CT FOR SOUTH

ANSWER

6c 73 d5 24 0a 94 8c 86 98 1b DF 94 86 4d 6d

Question 4 Mallability in OTP Attack