Kieren Ng

Cybersecurity Homework 2

1/31/18

**Not in book:**

1a. Neither

1b. Neither

1c. Read

1d. Read

1e. Neither

2a.

‘qeb mxpptloa fp nnwwnnw’

Q, E, B, M, X, T, L, O, A, F= 1/20 = 0.05

P, W= 3/20 = 0.15

N= 4/20 = 0.2

φ(*i*) = 0.05p(16-*i*) + 0.05p(4-*i*) + 0.05p(1-*i*) + 0.05p(12-*i*) + 0.05p(23-*i*) + 0.05p(19-*i*)

+ 0.05p(11-*i*) + 0.05p(14-*i*) + 0.05p(0-*i*) + 0.05p(5-*i*) + 0.15p(15-*i*) + 0.15p(22-*i*) +

0.2p(13-*i*)

|  |  |  |  |
| --- | --- | --- | --- |
| φ | φ (*i*) | φ | φ (*i*) |
| 0 (A) | 0.044 | 13 (N) | 0.040 |
| 1 (B) | 0.042 | 14 (O) | 0.029 |
| 2 (C) | 0.036 | 15 (P) | 0.041 |
| 3 (D) | 0.033 | 16 (Q) | 0.022 |
| 4 (E) | 0.035 | 17 (R) | 0.022 |
| 5 (F) | 0.042 | 18 (S) | 0.040 |
| 6 (G) | 0.028 | 19 (T) | 0.043 |
| 7 (H) | 0.035 | 20 (U) | 0.040 |
| 8 (I) | 0.049 | 21 (V) | 0.032 |
| **9 (J)** | **0.058** | **22 (W)** | **0.056** |
| 10 (K) | 0.034 | 23 (X) | 0.042 |
| **11 (L)** | **0.050** | 24 (Y) | 0.035 |
| 12 (M) | 0.039 | 25 (Z) | 0.032 |

2b.

‘the password is qqzzqqz’

Actual key = 23

2c. The actual key wasn’t part of the most likely keys, this is probably because the nonsense password skewed the correct likeliness.

**Review Questions**

2.4. Symmetric encryption, public-key encryption, secret value

2.7. Can be applied to a block of data any size, produces a fixed length output, H(x) is relatively easy to compute for any given x, One-way or pre-image resistant, computationally infeasible to find y!=x such that H(y) = H(x), Collision resistant or strong collision resistance

**Chapter 2 problems**

2.1. There is a flaw- you can undo the XOR if you have the random value by itself in this case. Since your partner is sending that value back as a confirmation, someone who might be listening in could get the key if they XOR again.

2.2a. Redundant letters need to be removed, so the second c in ‘cryptographic’ will be removed, for example.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C (2) | R (8) | Y (10) | P (7) | T (9) | O (6) | G (3) | A (1) | H (4) | I (5) |
| B | E | A | T | T | H | E | T | H | I |
| R | D | P | I | L | L | A | R | F | R |
| O | M | T | H | E | L | E | F | T | O |
| U | T | S | I | D | E | T | H | E | L |
| Y | C | E | U | M | T | H | E | A | T |
| R | E | T | O | N | I | G | H | T | A |
| T | S | E | V | E | N | I | F | Y | O |
| U | A | R | E | D | I | S | T | R | U |
| S | T | F | U | L | B | R | I | N | G |
| T | W | O | F | R | I | E | N | D | S |

‘TRFHE HFTIN BROUY RTUST EAETH GISRE HFTEA TYRND IROLT AOUGS HLLET INIBI TIHIU OVEUF EDMTC ESATW TLEDM NEDLR APTSE TERFO’

‘Network Security’ changed to ‘networkscuiy’ truncated to 10 characters to ‘networkscu’ (very relevant name tbh)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| N (4) | E (2) | T (8) | W (10) | O (5) | R (6) | K (3) | S (7) | C (1) | U (9) |
| T | R | F | H | E | H | F | T | I | N |
| B | R | O | U | Y | R | T | U | S | T |
| E | A | E | T | H | G | I | S | R | E |
| H | F | T | E | A | T | Y | R | N | D |
| I | R | O | L | T | A | O | U | G | S |
| H | L | L | E | T | I | N | I | B | I |
| T | I | H | I | U | O | V | E | U | F |
| E | D | M | T | C | E | S | A | T | W |
| T | L | E | D | M | N | E | D | L | R |
| A | P | T | S | E | T | E | R | F | O |

“ISRNG BUTLF RRAFR LIDLP FTIYO NVSEE TBEHI HTETA EYHAT TUCME HRGTA IOENT TUSRU IEADR FOETO LHMET NTEDS IFWRO HUTEL EITDS’

2.3a. P = (C-K1) XOR K2