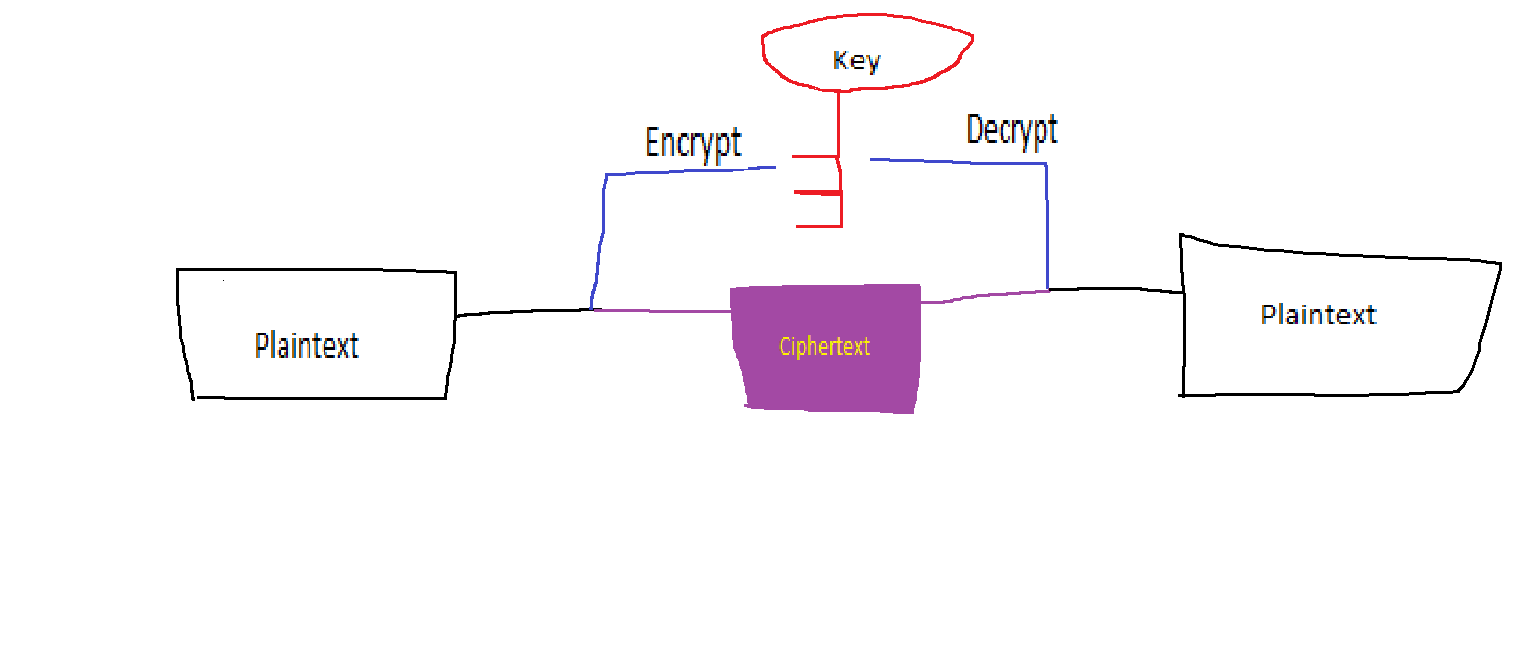
Ryan Carey

SRA 211

RUC230



2. AT LEAST C, but ideally G. There are open source encryption methods that reveal the encryption and/or decryption algorithm, but are still secure.

3. CTEXT = CATTIGER: PLAINTEXT = CIPTHERTEXT - KEY

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| C = 2 | A = 0 | T = 19 | T = 19 | I = 8 | G = 6 | E = 4 | R = 17 |
| S = 18 | U = 20 | N = 13 | S = 18 | U = 20 | N = 13 | S = 18 | U = 20 |
| 2  -18  +26  =10=K | 0  -20  +26  =6=G | 19  -13  =6=G | 19  -18  =1=B | 8  -20  +26  =14=O | 6  -13  +26  =19=T | 4  -18  +26  =12=M | 17  -20  +26  =23=X |

Plaintext = KGGBOTMX

4. PTEXT = HORSELSP: KEY = CTEXT – PTEXT

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| C = 2 | A = 0 | T = 19 | T = 19 | I = 8 | G = 6 | E = 4 | R = 17 |
| H = 7 | O = 14 | R = 17 | S = 18 | E = 4 | L = 11 | S = 18 | P = 15 |
| 2  -7  +26  =21=V | 0  -14  +26  =12=M | 19  -17  =2=C | 19  -18  =1=B | 8  -4  =4=E | 6  -11  +26  =21=V | 4  -18  +26  =12=M | …True that it’s repeating block size 5 |

Key = VMCBE

5. FALSE: The attacker finds out the plaintext of some chosen ciphertext and seeks to discover the key by finding some relationship between the ciphertext and plaintext.

Key = Ciphertext (ALGORITHM) plaintext : Find algorithm. In class we used addition and subtraction for the simplest possible example.