PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

APPLIED CRYPTOGRAPHY

Lecture 9

One time pad

Perfect secret system!!

One-time pad

- Patented in 1917 by Vernam
  - Recent historical research indicates it was invented (at least) 35 years earlier

- Proven perfectly secret by Shannon (1949)

One-time pad

- Let $\mathcal{M} = \{0,1\}^n$
- Gen: choose a uniform key $k \in \{0,1\}^n$
- $\text{Enc}_k(m) = k \oplus m$
- $\text{Dec}_k(c) = k \oplus c$

- Correctness:
  $$\begin{aligned} \text{Dec}_k(\ \text{Enc}_k(m)\ ) &= k \oplus (k \oplus m) \\ &= (k \oplus k) \oplus m = m \end{aligned}$$

Working Mechanism

- The encryption-key has at least the same length as the plaintext and consists of truly random numbers
- Each letter of the plaintext is 'mixed' with one element from the random number which is chosen from one-time password(OTP)
- This results in a ciphertext that has no relation with the plaintext when the key is unknown. At the receiving end, the same OTP is used to retrieve the original plaintext

One-Time Pad

- Let Z_m ={0,1,…,m-1} be
- the alphabet.

- Plaintext space = Ciphtertext space = Key space = $(Z_m)^n$
- The key is chosen uniformly randomly
- Plaintext X = $(x_1\ x_2\ \ldots\ x_n)$
- Key K = $(k_1\ k_2\ \ldots\ k_n)$
- Ciphertext Y = $(y_1\ y_2\ \ldots\ y_n)$
- $e_k(X) = (x_1+k_1\ \ x_2+k_2\ \ldots\ x_n+k_n)$ mod m
- $d_k(Y) = (y_1-k_1\ \ \ y_2-k_2\ \ldots\ \ y_n-k_n)$ mod m

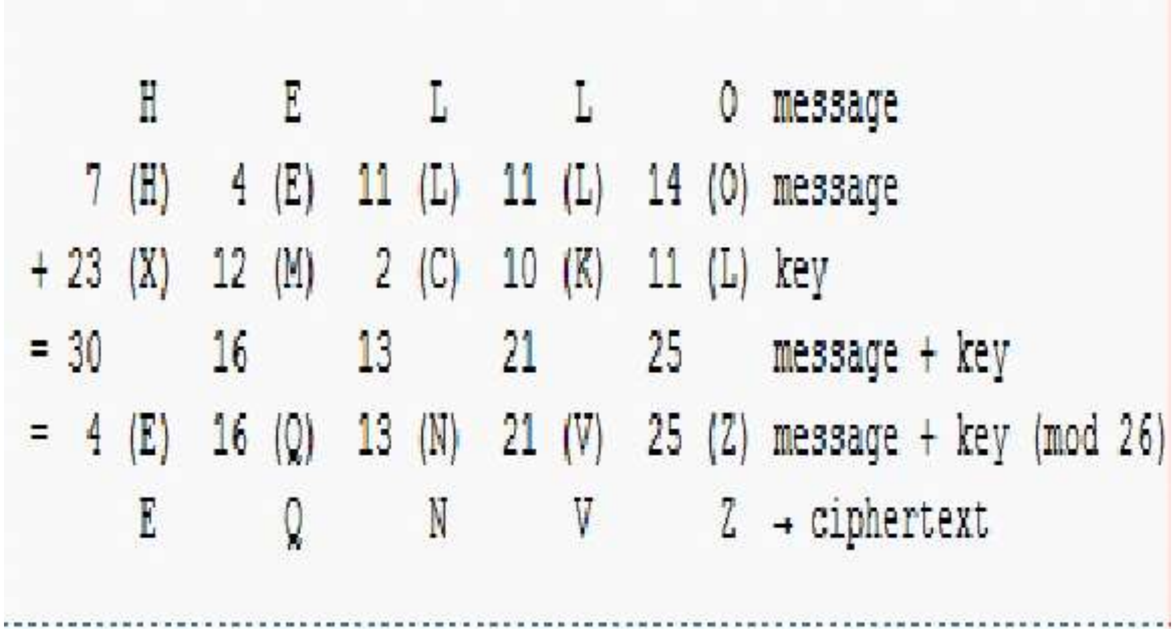
OTP Rules

- The OTP should consist of truely random numbers
- Precisely two copies of the OTP should exist.
- The OTP should only be used once.
- Both copies of the OTP are destroyed immediately after use.

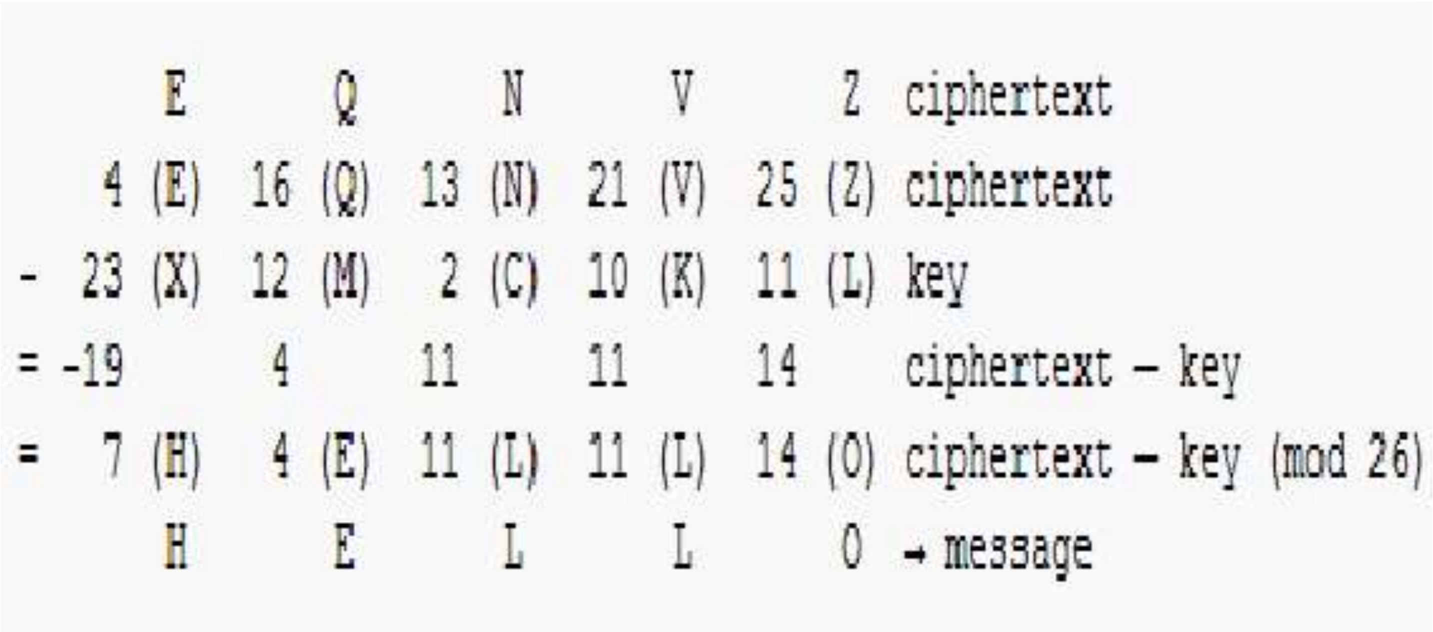
OTP is Unbreakable

- The key is atleast as long as the message
- The key is truly random (not auto-generated)
- Each key should only be used once & destroyed by sender and receiver
- There should only be 2 copies of the key

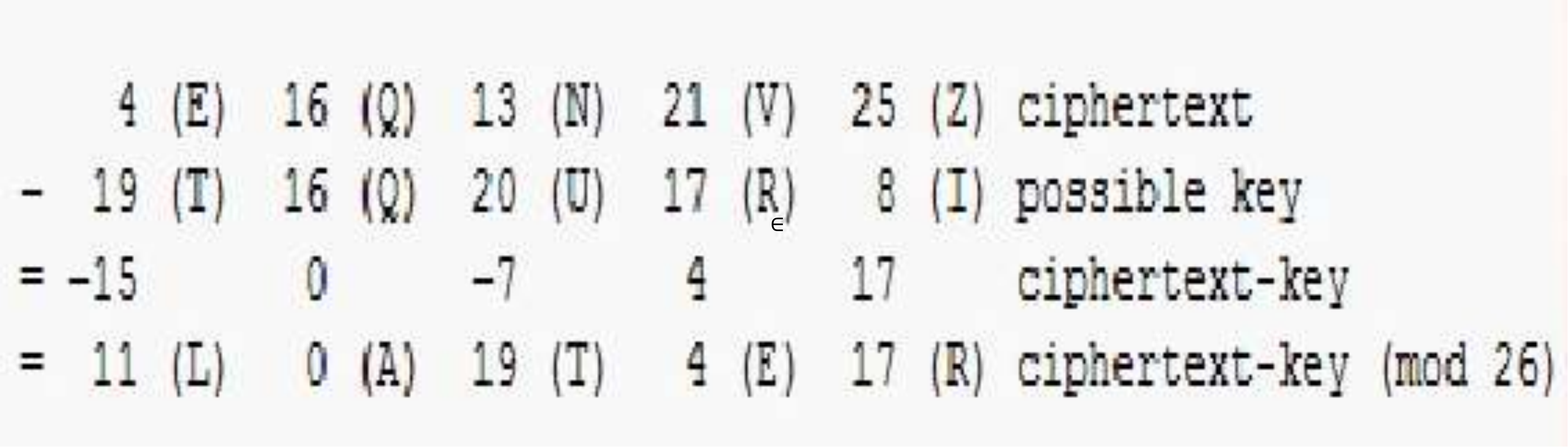
(1 for sender and 1 for receiver)



```
      H        E        L        L        O  message
   7 (H)    4 (E)   11 (L)   11 (L)   14 (O) message
+ 23 (X)   12 (M)    2 (C)   10 (K)   11 (L) key
= 30       16       13       21       25     message + key
=  4 (E)   16 (Q)   13 (N)   21 (V)   25 (Z) message + key (mod 26)
      E        Q        N        V        Z → ciphertext
```



```
       E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext – key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext – key  (mod 26)
       H       E       L       L       O  → message
```



```
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  19 (T)  16 (Q)  20 (U)  17 (R)   8 (I) possible key
= -15       0      -7       4      17     ciphertext-key
=  11 (L)   0 (A)  19 (T)   4 (E)  17 (R) ciphertext-key (mod 26)
```

Next Class

- ☞ Mandatory reading for the next class
- ☞ https://ieeexplore.ieee.org/document/7983647

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PESU IoT

PESU Center for
Internet
of Things