# CS 344: Operating Systems I

# 02.22: Part III – One-time pad (OTP)

M/W 12:00 – 1:50 PM (LINC #200)

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL
Secure AI Systems Lab

# Notice

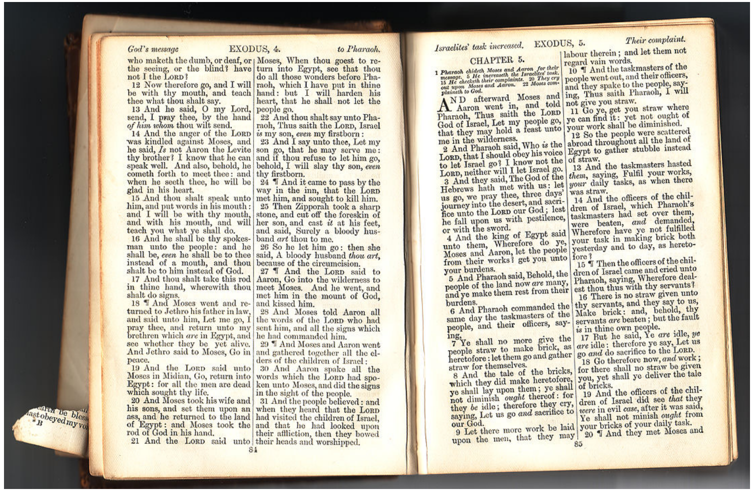
- Announcements
  - No lecture on the 27th
    - A slot for quizzes, assignments, and extra opportunities
    - SH will be on Discord
  - 2 more extra credit opportunities on Canvas
    - Build an ML classifier (+2%)
    - Multi-process data loader (+3%)
  - Programming assignment III

# Topics for today

- Part III: One-time pad (OTP)
  - OTP
    - What is it?
    - How does it work?
  - OTP in PA IV
    - What do we need to do?
    - Recap: client-server programming
  - OTP in the real-world

# One-time pad

- **OTP Example**
  - Password: _ _ _ _ (4-digit numbers)
  - Hint:
    - “keep on loving each other as brothers”
    - “fear not, for I am with you”
    - “You will not certainly die,” the serpent said
    - “Behold, I have told you before”



*God's message* EXODUS, 4. *to Pharaoh.*

who maketh the dumb, or deaf, or the seeing, or the blind? have not I the LORD?

12 Now therefore go, and I will be with thy mouth, and teach thee what thou shalt say.

13 And he said, O my Lord, send, I pray thee, by the hand *of him whom* thou wilt send.

14 And the anger of the LORD was kindled against Moses, and he said, *Is* not Aaron the Levite thy brother? I know that he can speak well. And also, behold, he cometh forth to meet thee: and when he seeth thee, he will be glad in his heart.

15 And thou shalt speak unto him, and put words in his mouth: and I will be with thy mouth, and with his mouth, and will teach you what ye shall do.

16 And he shall be thy spokesman unto the people: and he shall be, *even* he shall be to thee instead of a mouth, and thou shalt be to him instead of God.

17 And thou shalt take this rod in thine hand, wherewith thou shalt do signs.

18 ¶ And Moses went and returned to Jethro his father in law, and said unto him, Let me go, I pray thee, and return unto my brethren which *are* in Egypt, and see whether they be yet alive. And Jethro said to Moses, Go in peace.

19 And the LORD said unto Moses in Midian, Go, return into Egypt: for all the men are dead which sought thy life.

20 And Moses took his wife and his sons, and set them upon an ass, and he returned to the land of Egypt: and Moses took the rod of God in his hand.

21 And the LORD said unto Moses, When thou goest to return into Egypt, see that thou do all those wonders before Pharaoh, which I have put in thine hand: but I will harden his heart, that he shall not let the people go.

22 And thou shalt say unto Pharaoh, Thus saith the LORD, Israel *is* my son, *even* my firstborn:

23 And I say unto thee, Let my son go, that he may serve me: and if thou refuse to let him go, behold, I will slay thy son, *even* thy firstborn.

24 ¶ And it came to pass by the way in the inn, that the LORD met him, and sought to kill him.

25 Then Zipporah took a sharp stone, and cut off the foreskin of her son, and cast *it* at his feet, and said, Surely a bloody husband *art* thou to me.

26 So he let him go: then she said, A bloody husband *thou art*, because of the circumcision.

27 ¶ And the LORD said to Aaron, Go into the wilderness to meet Moses. And he went, and met him in the mount of God, and kissed him.

28 And Moses told Aaron all the words of the LORD who had sent him, and all the signs which he had commanded him.

29 ¶ And Moses and Aaron went and gathered together all the elders of the children of Israel:

30 And Aaron spake all the words which the LORD had spoken unto Moses, and did the signs in the sight of the people.

31 And the people believed: and when they heard that the LORD had visited the children of Israel, and that he had looked upon their affliction, then they bowed their heads and worshipped.

84

*Israelites' task increased.* EXODUS, 5. *Their complaint.*

CHAPTER 5.

*1 Pharaoh chideth Moses and Aaron for their message. 5 He increaseth the Israelites' task. 15 He checketh their complaints. 20 They cry out upon Moses and Aaron. 22 Moses complaineth to God.*

AND afterward Moses and Aaron went in, and told Pharaoh, Thus saith the LORD God of Israel, Let my people go, that they may hold a feast unto me in the wilderness.

2 And Pharaoh said, Who *is* the LORD, that I should obey his voice to let Israel go? I know not the LORD, neither will I let Israel go.

3 And they said, The God of the Hebrews hath met with us: let us go, we pray thee, three days' journey into the desert, and sacrifice unto the LORD our God; lest he fall upon us with pestilence, or with the sword.

4 And the king of Egypt said unto them, Wherefore do ye, Moses and Aaron, let the people from their works? get you unto your burdens.

5 And Pharaoh said, Behold, the people of the land now *are* many, and ye make them rest from their burdens.

6 And Pharaoh commanded the same day the taskmasters of the people, and their officers, saying,

7 Ye shall no more give the people straw to make brick, as heretofore: let them go and gather straw for themselves.

8 And the tale of the bricks, which they did make heretofore, ye shall lay upon them; ye shall not diminish *ought* thereof: for they *be* idle; therefore they cry, saying, Let us go *and* sacrifice to our God.

9 Let there more work be laid upon the men, that they may labour therein; and let them not regard vain words.

10 ¶ And the taskmasters of the people went out, and their officers, and they spake to the people, saying, Thus saith Pharaoh, I will not give you straw.

11 Go ye, get you straw where ye can find it: yet not ought of your work shall be diminished.

12 So the people were scattered abroad throughout all the land of Egypt to gather stubble instead of straw.

13 And the taskmasters hasted *them*, saying, Fulfil your works, *your* daily tasks, as when there was straw.

14 And the officers of the children of Israel, which Pharaoh's taskmasters had set over them, were beaten, *and* demanded, Wherefore have ye not fulfilled your task in making brick both yesterday and to day, as heretofore?

15 ¶ Then the officers of the children of Israel came and cried unto Pharaoh, saying, Wherefore dealest thou thus with thy servants?

16 There is no straw given unto thy servants, and they say to us, Make brick: and, behold, thy servants *are* beaten; but the fault *is* in thine own people.

17 But he said, Ye *are* idle, *ye are* idle: therefore ye say, Let us go *and* do sacrifice to the LORD.

18 Go therefore now, *and* work; for there shall no straw be given you, yet shall ye deliver the tale of bricks.

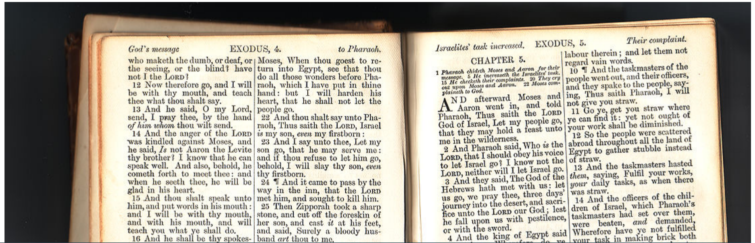
19 And the officers of the children of Israel did see *that* they *were* in evil *case*, after it was said, Ye shall not minish *ought* from your bricks of your daily task.

20 ¶ And they met Moses and

85

# One-time pad

- **OTP Example**
  - Password: _ _ _ _ (4-digit numbers)
  - Hint:
    - "keep on loving each other as brothers"
    - "fear not, for I am with you"
    - "You will not certainly die," the serpent said
    - "Behold, I have told you before"
  - Solution: 4 2 5 0
    - "keep … " > Hebrews > 13: **4**
    - "fear n…" > Isaiah > 66: **2**
    - "You w…" > Genesis > 50: **5**
    - "Behol…" > Matthew > 28: **0**



*God's message* EXODUS, 4. *to Pharaoh.*

who maketh the dumb, or deaf, or the seeing, or the blind? have not I the LORD?

12 Now therefore go, and I will be with thy mouth, and teach thee what thou shalt say.

13 And he said, O my Lord, send, I pray thee, by the hand *of him whom* thou wilt send.

14 And the anger of the LORD was kindled against Moses, and he said, *Is* not Aaron the Levite thy brother? I know that he can speak well. And also, behold, he cometh forth to meet thee: and when he seeth thee, he will be glad in his heart.

15 And thou shalt speak unto him, and put words in his mouth: and I will be with thy mouth, and with his mouth, and will teach you what ye shall do.

16 And he shall be thy spokes-

Moses, When thou goest to return into Egypt, see that thou do all those wonders before Pharaoh, which I have put in thine hand: but I will harden his heart, that he shall not let the people go.

22 And thou shalt say unto Pharaoh, Thus saith the LORD, Israel *is* my son, *even* my firstborn:

23 And I say unto thee, Let my son go, that he may serve me: and if thou refuse to let him go, behold, I will slay thy son, *even* thy firstborn.

24 ¶ And it came to pass by the way in the inn, that the LORD met him, and sought to kill him.

25 Then Zipporah took a sharp stone, and cut off the foreskin of her son, and cast *it* at his feet, and said, Surely a bloody husband *art* thou to me.

*Israelites' task increased.* EXODUS, 5. *Their complaint.*

CHAPTER 5.

1 *Pharaoh chideth Moses and Aaron for their message. 5 He increaseth the Israelites' task. 15 He checketh their complaints. 20 They cry out upon Moses and Aaron. 22 Moses complaineth to God.*

AND afterward Moses and Aaron went in, and told Pharaoh, Thus saith the LORD God of Israel, Let my people go, that they may hold a feast unto me in the wilderness.

2 And Pharaoh said, Who *is* the LORD, that I should obey his voice to let Israel go? I know not the LORD, neither will I let Israel go.

3 And they said, The God of the Hebrews hath met with us: let us go, we pray thee, three days' journey into the desert, and sacrifice unto the LORD our God; lest he fall upon us with pestilence, or with the sword.

4 And the king of Egypt said

labour therein; and let them not regard vain words.

10 ¶ And the taskmasters of the people went out, and their officers, and they spake to the people, saying, Thus saith Pharaoh, I will not give you straw.

11 Go ye, get you straw where ye can find it: yet not ought of your work shall be diminished.

12 So the people were scattered abroad throughout all the land of Egypt to gather stubble instead of straw.

13 And the taskmasters hasted *them*, saying, Fulfil your works, *your* daily tasks, as when there was straw.

14 And the officers of the children of Israel, which Pharaoh's taskmasters had set over them, were beaten, *and* demanded, Wherefore have ye not fulfilled your task in making brick both

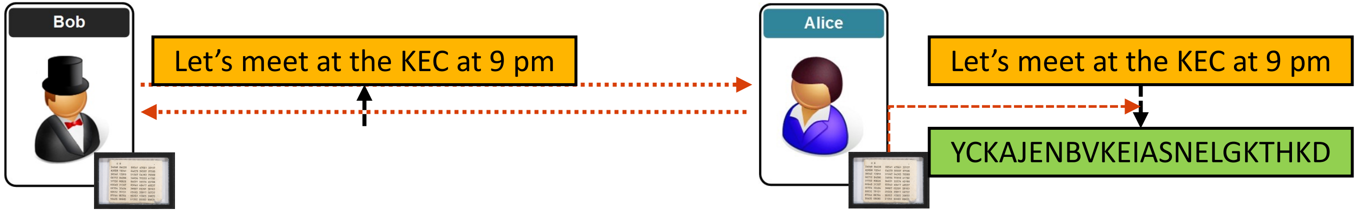
# One-time pad

- **What is it?**
  - <u>O</u>ne-<u>T</u>ime <u>P</u>ads (**<u>OTP</u>**) is an encryption mechanism

- **How it works?**
  - Alice and Bob want to communicate *securely*
  - Alice and Bob share the same OTP
  - Alice encrypts a message to send with the OTP
  - Alice sends the encrypted message to Bob
  - Bob decrypts the received message with the OTP

```
   0 8
54048 84038   99541 47661 32157
83268 19341   64279 92507 97500
58542 13918   01247 64383 79389
68712 94286   54894 70559 41792
57752 80626   94691 55574 45188
82649 31307   83240 49417 48537
02724 32494   38807 05391 58183
90032 78151   25665 35817 02737
97244 86764   96263 10925 30877
56426 08685   61282 99993 8983
```

**An Example OTP**



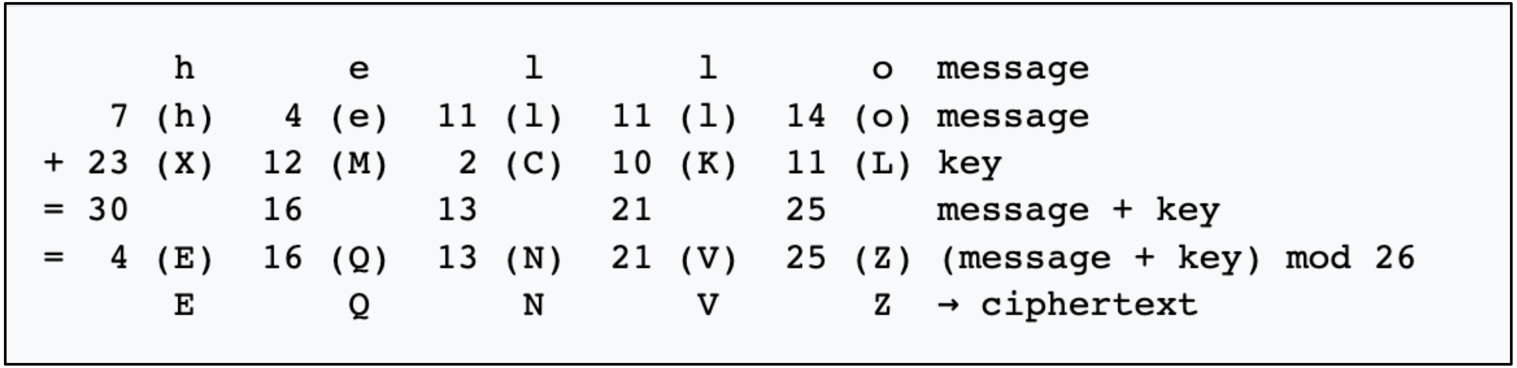
Let’s meet at the KEC at 9 pm

Let’s meet at the KEC at 9 pm

YCKAJENBVKEIASNELGKTHKD

# One-time pad: encryption

- **Encryption example**
  - Taken from Wikepedia (link)
  - Alice wants to say “hello” to Bob
    (Key chosen from OTP: XMCKL)



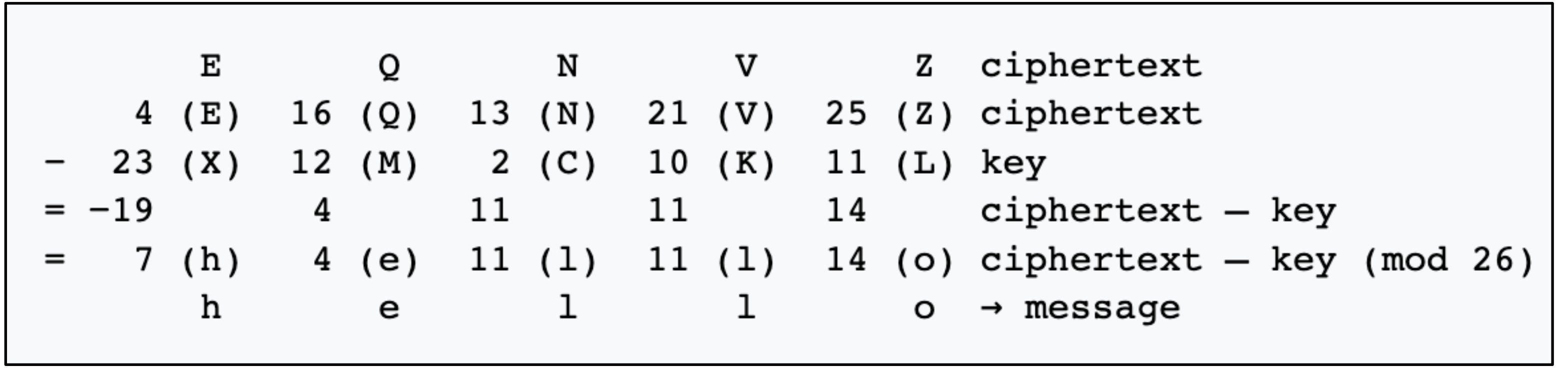
```
        h          e          l          l          o   message
     7 (h)      4 (e)     11 (l)     11 (l)     14 (o)  message
 + 23 (X)     12 (M)      2 (C)     10 (K)     11 (L)  key
 = 30          16         13         21         25      message + key
 =   4 (E)    16 (Q)     13 (N)     21 (V)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

  - Alice’s “hello” becomes “EQNVZ”
  - Alice sends “EQNVZ” to Bob
  - **Enc(m, k) := [(m + k) mod 26]**

**EQNVZ:** Ciphertext (the output of an encryption)
**hello** **:** Plaintext (the text we want to encrypt)
**XMCKL:** Key (the text we use for the encryp-/decryption)

# One-time pad: decryption

- **Decryption example**
  - Bob receives “EQNVZ” from Alice
  - Bob has the same key chosen from OTP (XMCKL)



```
        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
```

  - Alice’s “EQNVZ” now becomes “hello”
  - **Dec(c, k) := [(c - k) mod 26]**

# Topics for today

- Part III: One-time pad (OTP)
  - OTP
    - What is it?
    - How does it work?
  - OTP in PA IV
    - What do we need to do?
    - Recap: client-server programming
  - OTP in the real-world

# One-time pad: programming assignment IV

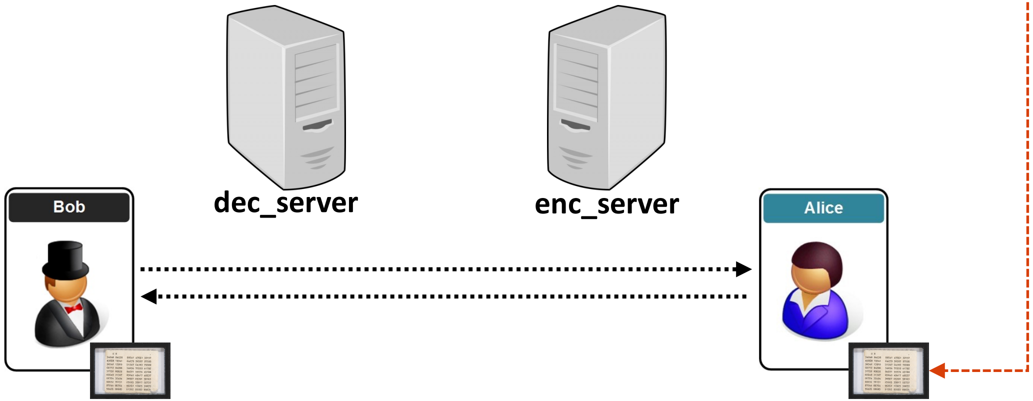
- **Required programs**
  - (keygen) Key generator
  - (enc_server) Encryption server
  - (enc_client) Encryption client
  - (dec_server) Decryption server
  - (dec_client) Decryption client

# One-time pad: programming assignment IV

- **Overall process**
  - (keygen) Alice generates a key via a keygen program
  - (keygen) Bob has the *same* key (do not re-generate)
  - Suppose there are two servers
    - (enc_server) Encrypt a plaintext using a key
    - (dec_server) Decrypt a ciphertext using a key

**(keygen)**
Input: key length (int)
Output: a *randomly* generated key

ex. $ ./keygen 10
QKASLKNGDK



# One-time pad: programming assignment IV

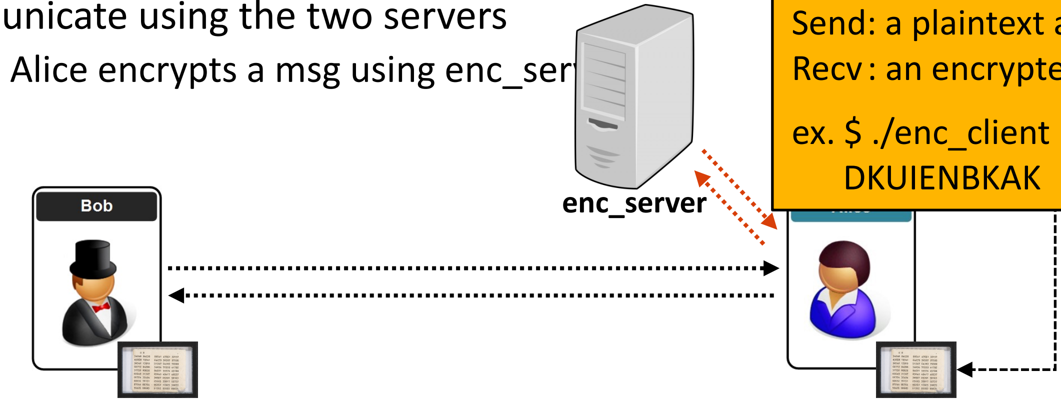
- **Overall process**
  - (keygen) Alice generates a key via a keygen program
  - (keygen) Bob has the *same* key (do not re-generate)
  - Suppose there are two servers
    - (enc_server) Encrypt a plaintext using a key
    - (dec_server) Decrypt a ciphertext using a key
  - Securely communicate using the two servers
    - (enc_client) Alice encrypts a msg using enc_ser

**(keygen)**
Input: key length (int)
Output: a *randomly* generated key

```
ex. $ ./keygen 10
      QKASLKNGDK
```

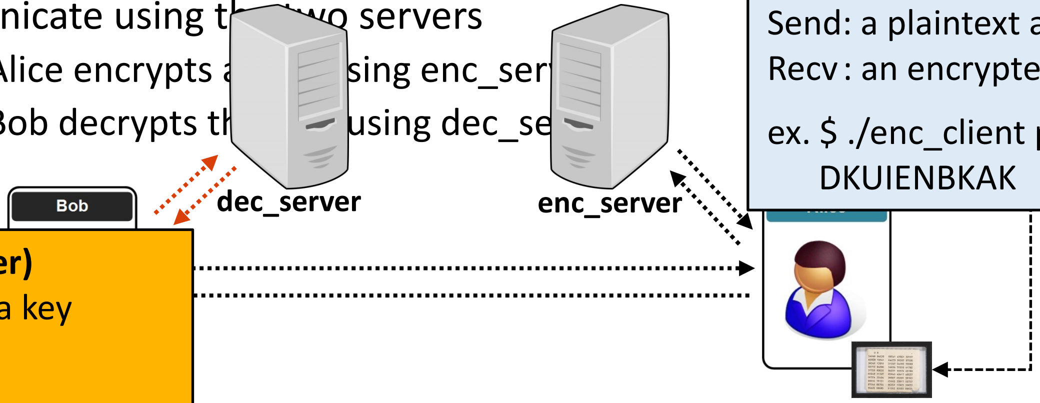
**(enc_client > enc_server)**
Send: a plaintext and a key
Recv : an encrypted text

```
ex. $ ./enc_client ptext key port
      DKUIENBKAK
```



# One-time pad: programming assignment IV

- **Overall process**
  - (keygen) Alice generates a key via a keygen program
  - (keygen) Bob has the *same* key (do not re-generate)
  - Suppose there are two servers
    - (enc_server) Encrypt a plaintext using a key
    - (dec_server) Decrypt a ciphertext using a key
  - Securely communicate using t wo servers
    - (enc_client) Alice encrypts a sing enc_ser
    - (dec_client) Bob decrypts th using dec_se



**(keygen)**
Input: key length (int)
Output: a *randomly* generated key

```
ex. $ ./keygen 10
    QKASLKNGDK
```

**(enc_client > enc_server)**
Send: a plaintext and a key
Recv : an encrypted text

```
ex. $ ./enc_client ptext key port
    DKUIENBKAK
```

**(dec_client > dec_server)**
Send: a ciphertext and a key
Recv : a plaintext

```
ex. $ ./dec_client ctext key port
    ptext
```

# Revisit networking: port

- Port
  - **Formal:** A communication endpoint (defined at the transport layer)
  - **TL; DR :** A number (0 – 65535) that must be associated with an IP for communication

- Notation
  - <IP address>:<Port number>
    - ex. 76.298.83.129:433
    - IP address: 76.298.83.129 | Port #: 443

- Ports reserved in Linux
  - 22: SSH connection
  - 80: HTTP
  - 443: HTTPS
  - 2967: Symantec AV
  - 6112: Battle.net

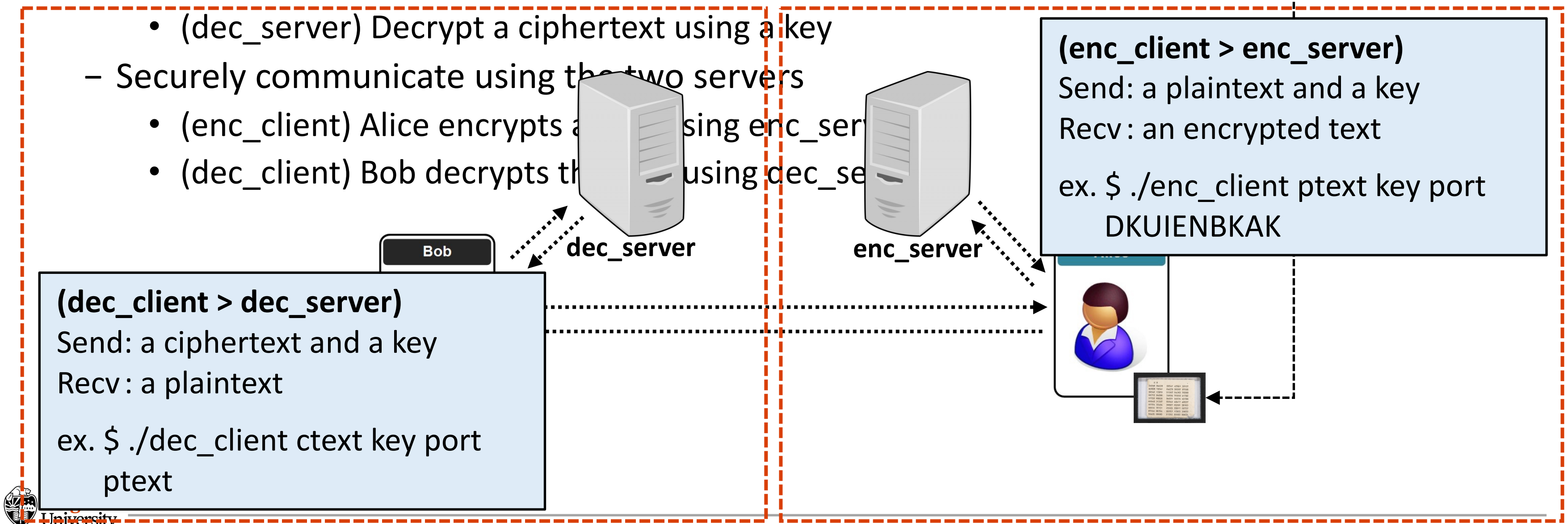
**Tip:**
- Use port # in the 50000+ range
- Use different port number every time you run the server
  [Note: it is still unavailable for some time after your program terminates]
- Oftentimes, a port is already used by your fellow; then choose others
- `$ netstat -tulp | grep LISTEN` (to see used ports)

# One-time pad: client-server architecture

- **OTP in PA V**
  - (keygen) Alice generates a key via a keygen program
  - (keygen) Bob has the *same* key (do not re-generate)
  - Suppose there are two servers
    - (enc_server) Encrypt a plaintext using a key
    - (dec_server) Decrypt a ciphertext using a key
  - Securely communicate using the two servers
    - (enc_client) Alice encrypts a sing enc_ser
    - (dec_client) Bob decrypts th using dec_se

**(keygen)**
Input: key length (int)
Output: a *randomly* generated key

ex. $ ./keygen 10
QKASLKNGDK



**(enc_client > enc_server)**
Send: a plaintext and a key
Recv : an encrypted text

ex. $ ./enc_client ptext key port
DKUIENBKAK

**(dec_client > dec_server)**
Send: a ciphertext and a key
Recv : a plaintext

ex. $ ./dec_client ctext key port
ptext

# Revisit: client-server programming (client.c)

```c
#define  IPADDR  <SERVER_IP>
#define  PORT     <SERVER_PORT>
#define  BUFSIZE 1024

int main(int argc, char *argv)
{
   int sock = 0, valread;
   struct sockaddr_in serv_addr;
   char* hello = "Hello (client)";
   char buffer[BUFSIZE] = { 0 };

// create a socket
if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0) {
   printf("Error: socket creation error\n");
   return -1;
}

serv_addr.sin_family = AF_INET;
serv_addr.sin_port = htons(PORT);

// convert IP addresses from text to binary
if (inet_pton(AF_INET, IPADDR, &serv_addr.sin_addr) <= 0) {
   printf("Error: invalid address, address not supported\n");
   return -1;
}
```

AF_INET (IPv4)
SOCK_STREAM (bi-directional)

```c
if (connect(sock, (struct sockaddr*)&serv_addr, sizeof(serv_addr)) < 0) {
   printf("Connection Failed\n");
   return -1;
}

// request encryption/decryption
 send(sock, hello, strlen(hello), 0);
 printf("Message sent (client)\n");
 valread = recv(sock, buffer, BUFSIZE);
 printf("%s\n", buffer);

 return 0;
}
```

Connect to the server, running on the IP address we specify “127.0.0.1”

**Our OTP case:**

1. Send a plan/ciphertext and a key
2. Receive a cipher/plaintext

# Revisit: client-server programming (server.c)

```
... omit the includes

#define  BUF_SIZE   1024
#define  PORT       SERVER_PORT

int main(void) {
    int server_fd, new_socket, valread;
    struct sockaddr_in address;
    int opt = 1;
    int addrlen = sizeof(address);
    char buffer[BUF_SIZE] = { 0 };
    char* hello = "Hello (server)!";

    // create socket (returns a file descriptor for read/write
    if ((server_fd = socket(AF_INET, SOCK_STREAM, 0)) == 0) {
        perror("socket failed"); exit(EXIT_FAILURE);
    }

    // (you can skip) attach this socket to the port number 8080
    if (setsockopt(server_fd, SOL_SOCKET,
                   SO_REUSEADDR | SO_REUSEPORT, &opt, sizeof(opt))) {
        perror("setsocketopt failed"); exit(EXIT_FAILURE);
    }

    address.sin_family = AF_INET;
    address.sin_addr.s_addr = INADDR_ANY;  // bind to any address
    address.sin_port = htons(PORT);        // format the port num

    // attach socket to the port 8080
    if (bind(server_fd, (struct sockaddr*)&address, sizeof(address)) < 0) {
        perror("bind failed"); exit(EXIT_FAILURE);
    }

    if (listen(server_fd, 3) < 0) {
        perror("listen failed"); exit(EXIT_FAILURE);
    }

    while (1) {
        if ((new_socket = accept(server_fd,
                                 (struct sockaddr*)&address,
                                 (socklen_t*)&sizeof(address))) < 0) {
            perror("accept");
            exit(EXIT_FAILURE);
        }

        valread = read(new_socket, buffer, 1024);
        printf("%s\n", buffer);
        send(new_socket, hello, strlen(hello), 0);
        printf("Message sent (server)\n");
        close(new_socket);
    }
    close(server_fd);
    return 0;
}
```

AF_INET (IPv4)
SOCK_STREAM (bi-directional)

SO_REUSEADDR
SO_REUSEPORT
opt (optional value)

Bind the socket to the address
> Any IP (of the host)
> Port # 8080

Listen incoming connections
> Use the socket fd
> Allow 3 connections (max.)

**Our OTP case:**

1. Receive a plan/ciphertext and a key
2. Send a cipher/plaintext

# Topics for today

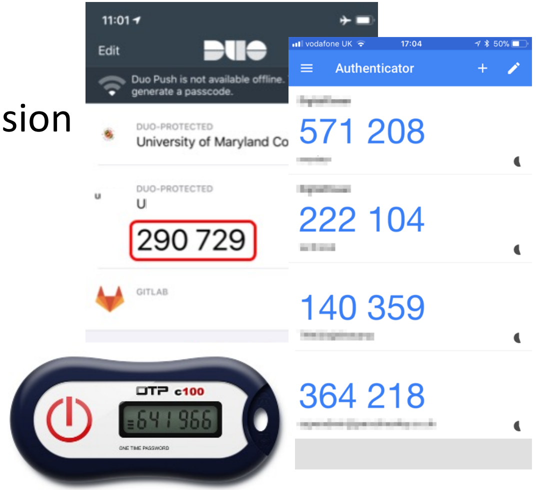
- Part III: One-time pad (OTP)
  - OTP
    - What is it?
    - How does it work?
  - OTP in PA IV
    - What do we need to do?
    - Recap: client-server programming
  - OTP in the real-world

# One-time pad: problems

- What if
  - Your key is not (completely) random?
  - An adversary knows the OTP you use?
  - An adversary observes both ciphertext and plaintext?
  - Someone implements OTP incorrectly?

# One-time password

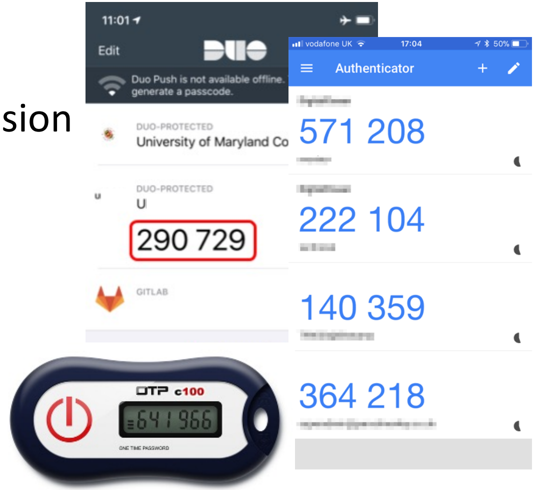
- **What is it?**
  - One-Time Password (**OTP**) is a password only valid for one session



Duo Push is not available offline. generate a passcode.

# One-time password

- **What is it?**
  - One-Time Password (**OTP**) is a password only valid for one session



11:01

Edit

DUO

Duo Push is not available offline. generate a passcode.

DUO-PROTECTED
University of Maryland Co

DUO-PROTECTED
U

290 729

GITLAB

vodafone UK 17:04 50%

Authenticator

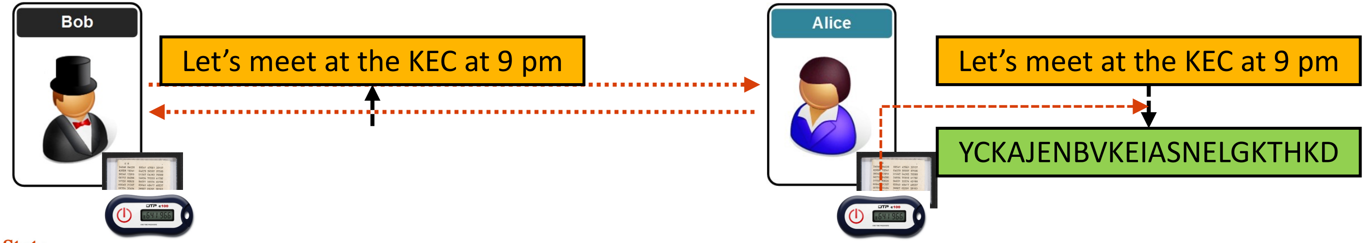
571 208

222 104

140 359

364 218

- **How it works?**
  - Alice and Bob want to communicate *securely*
  - Alice and Bob share the same OTP (for **only one** session)
  - Alice encrypts a message to send with the OTP
  - Alice sends the encrypted message to Bob
  - Bob decrypts the received message with the OTP



Bob

Let's meet at the KEC at 9 pm

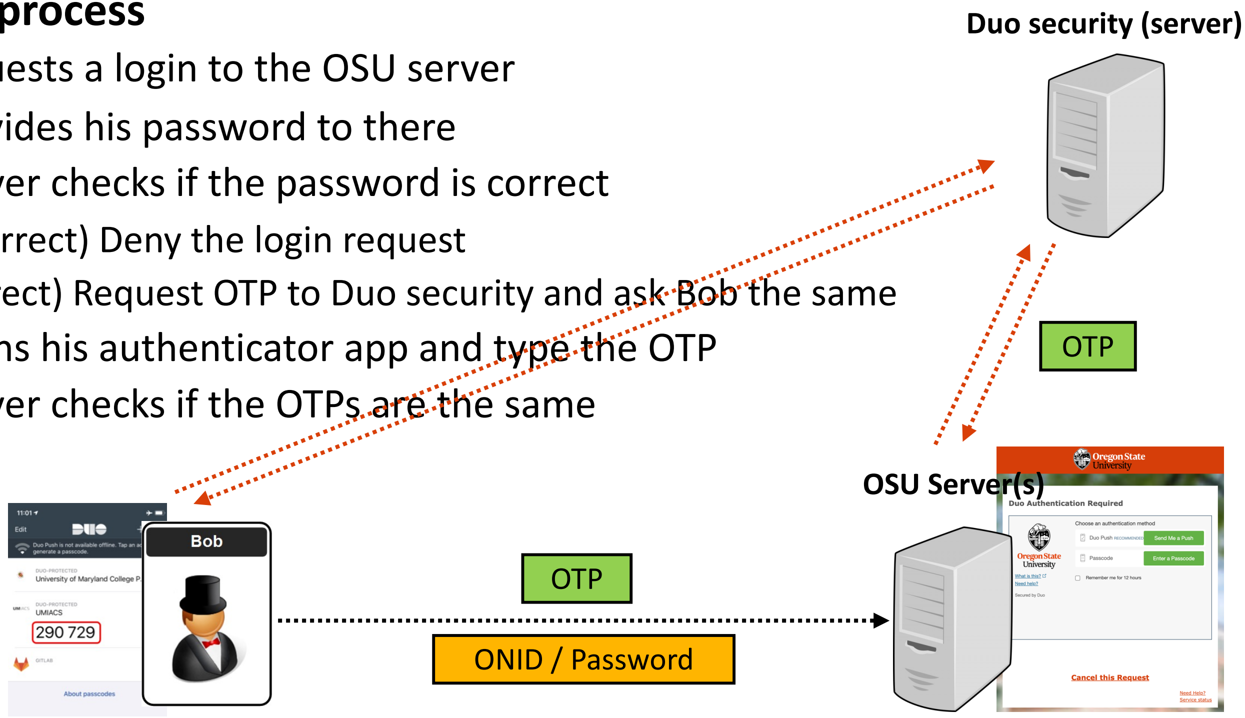
Alice

Let's meet at the KEC at 9 pm

YCKAJENBVKEIASNELGKTHKD

# One-time password

- **OSU log-in process**
  - Bob requests a login to the OSU server
  - Bob provides his password to there
  - OSU server checks if the password is correct
    - (Incorrect) Deny the login request
    - (Correct) Request OTP to Duo security and ask Bob the same
  - Bob opens his authenticator app and type the OTP
  - OSU server checks if the OTPs are the same

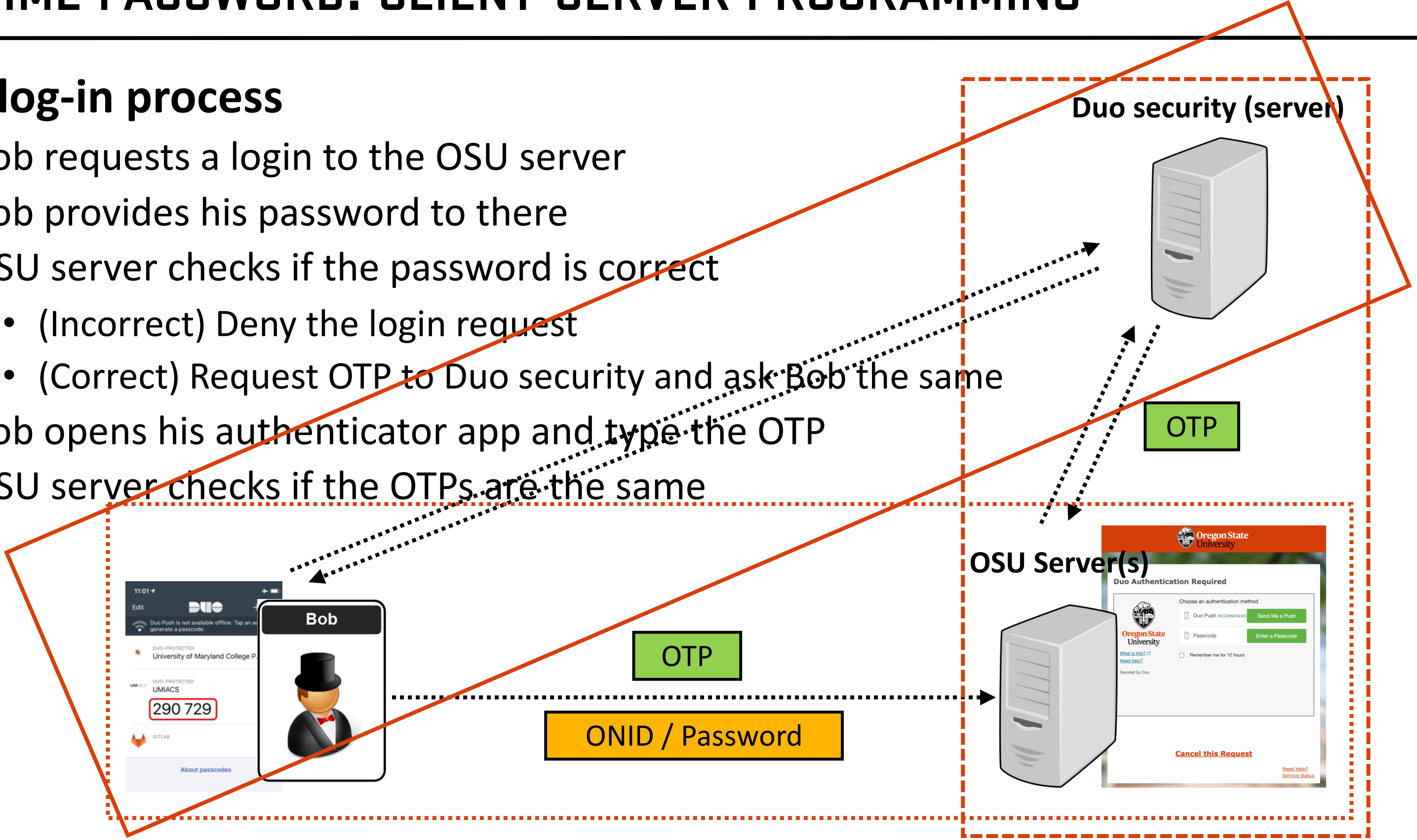


11:01
Edit
DUO
Duo Push is not available offline. Tap an ac generate a passcode.
DUO-PROTECTED
University of Maryland College P
DUO-PROTECTED
UMIACS
290 729
GITLAB
About passcodes

Oregon State University
Duo Authentication Required
Choose an authentication method
Duo Push RECOMMENDED — Send Me a Push
Passcode — Enter a Passcode
□ Remember me for 12 hours
What is this?
Need help?
Secured by Duo
Cancel this Request
Need Help?
Service status

# One-time password: client-server programming

- **OSU log-in process**
  - Bob requests a login to the OSU server
  - Bob provides his password to there
  - OSU server checks if the password is correct
    - (Incorrect) Deny the login request
    - (Correct) Request OTP to Duo security and ask Bob the same
  - Bob opens his authenticator app and type the OTP
  - OSU server checks if the OTPs are the same



Duo Push is not available offline. Tap an ac generate a passcode.

Duo Authentication Required

Choose an authentication method

□ Remember me for 12 hours

# Topics for today

- Part III: One-time pad (OTP)
  - OTP
    - What is it?
    - How does it work?
  - OTP in PA IV
    - What do we need to do?
    - Recap: client-server programming
  - OTP in the real-world

# Thank You!

M/W 12:00 – 1:50 PM (LINC #200)

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL

Secure AI Systems Lab