

CS 105

Week 13

Midterm 2 (Multiple Choice Only)

Median: 87.5% (28/32)

Average: 83.6% (26.8/32)

48 Perfect Scores

Midterm 2

FR Grading in Progress
(Grades expected on Wednesday)



Project Proposal

Lab Sections on Nov. 12-14



Project Update

Lab Sections on Nov. 19-21

Project Due Date

Lab Sections on Dec. 3-5

Final Project

In Lab: Demo your project to TAs

(This is what you will be graded on)

Final Project

In Lab: Demo your project to TAs

Website (by Sat, 5pm): Upload your project to the CS 105 website with a screenshot

Cyber Monday

Thanksgiving Day

Black Friday

Small Business Saturday

??

Cyber Monday

SSL

SSL

Secure Sockets Layer

SSL “v2” →

SSL “v2” → TLS

TLS

Transport Layer Security



<https://courses.engr.illinois.edu/cs105/>



<https://courses.engr.illinois.edu/cs105/>



Page Info - <https://courses.engr.illinois.edu/cs105/>



General



Permissions



Security

Website Identity

Website: **courses.engr.illinois.edu**

Owner: **This website does not supply ownership information.**

Verified by: **Internet2**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? **Yes, 1,280 times**

Is this website storing information (cookies) on my computer? **Yes**

[View Cookies](#)

Have I saved any passwords for this website? **No**

[View Saved Passwords](#)

Technical Details

Connection Encrypted: High-grade Encryption (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

9b	68	6c	11	7e	55	71	82	cd	20	58	78	2d	15	0f	09
5d	04	05	56	ea	d2	3b	3b	12	a7	eb	fd	23	3a	c3	fb
c8	01	98	2b	32	06	72	2c	12	f9	0d	ee	1c	01	02	23
40	a5	1a	d7	ec	56	02	72	13	38	69	41	05	22	64	8a
4e	43	90	ae	8a	df	38	b8	d0	29	9d	f7	5b	3e	1f	80
f7	ef	17	50	05	be	ff	2f	47	7e	99	26	19	c7	7c	b7
6a	b4	ac	35	c2	91	fc	2d	26	ad	d3	63	76	de	3c	09
6b	8d	94	4c	9b	6a	24	1b	03	8c	3b	c3	10	67	65	ca
03	b1	a2	25	3c	1c	2a	90	7e	49	e4	45	67	b2	5a	54
34	97	6e	1b	7b	5f	c4	d1	b1	a5	1a	d6	a5	67	6e	ca
1e	6f	b9	85	ff	3c	44	2b	cd	d6	f8	ea	f9	d3	46	de
8f	bd	dd	d9	36	fd	50	81	fb	71	72	b0	62	47	6c	91
bd	6e	bd	3f	be	54	2f	c9	ec	51	16	5e	c3	77	44	a3
40	63	3e	b6	38	7f	81	a0	50	7f	81	d3	a5	7b	7c	1f
a6	09	9f	a1	e9	62	44	d0	f8	83	28	9a	ae	be	3f	03
51	8c	67	51	f9	5b	3a	68	2c	37	9a	b3	1c	49	4f	9b

0 → 0000

1 → 0001

2 → 0010

3 → 0011

4 → 0100

5 → 0101

6 → 0110

7 → 0111

8 → 1000

9 → 1001

a → 1010

b → 1011

c → 1100

d → 1101

e → 1110

f → 1111

1001b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09

5d	04	05	56	ea	d2	3b	3b	12	a7	eb	fd	23	3a	c3	fb
c8	01	98	2b	32	06	72	2c	12	f9	0d	ee	1c	01	02	23
40	a5	1a	d7	ec	56	02	72	13	38	69	41	05	22	64	8a
4e	43	90	ae	8a	df	38	b8	d0	29	9d	f7	5b	3e	1f	80
f7	ef	17	50	05	be	ff	2f	47	7e	99	26	19	c7	7c	b7
6a	b4	ac	35	c2	91	fc	2d	26	ad	d3	63	76	de	3c	09
6b	8d	94	4c	9b	6a	24	1b	03	8c	3b	c3	10	67	65	ca
03	b1	a2	25	3c	1c	2a	90	7e	49	e4	45	67	b2	5a	54
34	97	6e	1b	7b	5f	c4	d1	b1	a5	1a	d6	a5	67	6e	ca
1e	6f	b9	85	ff	3c	44	2b	cd	d6	f8	ea	f9	d3	46	de
8f	bd	dd	d9	36	fd	50	81	fb	71	72	b0	62	47	6c	91
bd	6e	bd	3f	be	54	2f	c9	ec	51	16	5e	c3	77	44	a3
40	63	3e	b6	38	7f	81	a0	50	7f	81	d3	a5	7b	7c	1f
a6	09	9f	a1	e9	62	44	d0	f8	83	28	9a	ae	be	3f	03
51	8c	67	51	f9	5b	3a	68	2c	37	9a	b3	1c	49	4f	9b

100110110110100001101100000100010111111001010101010111000110000010
1100110100100000010110000111100000101101000101010000111100001001

5d	04	05	56	ea	d2	3b	3b	12	a7	eb	fd	23	3a	c3	fb
c8	01	98	2b	32	06	72	2c	12	f9	0d	ee	1c	01	02	23
40	a5	1a	d7	ec	56	02	72	13	38	69	41	05	22	64	8a
4e	43	90	ae	8a	df	38	b8	d0	29	9d	f7	5b	3e	1f	80
f7	ef	17	50	05	be	ff	2f	47	7e	99	26	19	c7	7c	b7
6a	b4	ac	35	c2	91	fc	2d	26	ad	d3	63	76	de	3c	09
6b	8d	94	4c	9b	6a	24	1b	03	8c	3b	c3	10	67	65	ca
03	b1	a2	25	3c	1c	2a	90	7e	49	e4	45	67	b2	5a	54
34	97	6e	1b	7b	5f	c4	d1	b1	a5	1a	d6	a5	67	6e	ca
1e	6f	b9	85	ff	3c	44	2b	cd	d6	f8	ea	f9	d3	46	de
8f	bd	dd	d9	36	fd	50	81	fb	71	72	b0	62	47	6c	91
bd	6e	bd	3f	be	54	2f	c9	ec	51	16	5e	c3	77	44	a3
40	63	3e	b6	38	7f	81	a0	50	7f	81	d3	a5	7b	7c	1f
a6	09	9f	a1	e9	62	44	d0	f8	83	28	9a	ae	be	3f	03
51	8c	67	51	f9	5b	3a	68	2c	37	9a	b3	1c	49	4f	9b

100110110110100001101100000100010111111001010101010111000110000010
1100110100100000010110000111100000101101000101010000111100001001
0101110100000100000001010101011011101010110100100011101100111011
000100101010011111101011111110100100011001110101100001111111011

c8	01	98	2b	32	06	72	2c	12	f9	0d	ee	1c	01	02	23
40	a5	1a	d7	ec	56	02	72	13	38	69	41	05	22	64	8a
4e	43	90	ae	8a	df	38	b8	d0	29	9d	f7	5b	3e	1f	80
f7	ef	17	50	05	be	ff	2f	47	7e	99	26	19	c7	7c	b7
6a	b4	ac	35	c2	91	fc	2d	26	ad	d3	63	76	de	3c	09
6b	8d	94	4c	9b	6a	24	1b	03	8c	3b	c3	10	67	65	ca
03	b1	a2	25	3c	1c	2a	90	7e	49	e4	45	67	b2	5a	54
34	97	6e	1b	7b	5f	c4	d1	b1	a5	1a	d6	a5	67	6e	ca
1e	6f	b9	85	ff	3c	44	2b	cd	d6	f8	ea	f9	d3	46	de
8f	bd	dd	d9	36	fd	50	81	fb	71	72	b0	62	47	6c	91
bd	6e	bd	3f	be	54	2f	c9	ec	51	16	5e	c3	77	44	a3
40	63	3e	b6	38	7f	81	a0	50	7f	81	d3	a5	7b	7c	1f
a6	09	9f	a1	e9	62	44	d0	f8	83	28	9a	ae	be	3f	03
51	8c	67	51	f9	5b	3a	68	2c	37	9a	b3	1c	49	4f	9b

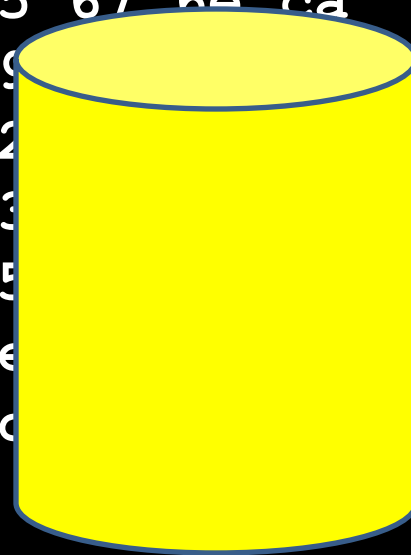
1001101101101000011011000001000101111110010101010111000110000010
1100110100100000010110000111100000101101000101010000111100001001
01011101000001000000010101010110111010101101001000111100111011
00010010101001111110101111111010010001100111011001111111011

c8	01	98	2b	32	06	72	2c	12	f9	0d	1c	01	02	23
40	a5	1a	d7	ec	56	02	72	38	69	41	05	22	64	8a
4e	43	90	ae	8a	df	38	b8	d1	19	d7	3e	1f	80	
f7	ef	17	50	05	be	2f	47	7e	90	20	19	c7	7c	b7
6a	b4	ac	35	c2	91	fc	2d	26	a1	43	63	76	de	3c
6b	8d	94	4c	90	6a	20	11	03	8c	3b	c3	10	67	65
03	b1	a5	35	3e	20	00	7e	49	e4	45	67	b2	5a	54
34	97	e1	70	c4	d1	b1	a5	1a	d6	a5	67	6e	ca	
fe	10	85	ff	3c	44	2b	cd	d6	f8	ea	f9	d3	46	de
8f	b1	dc	d0	36	fd	50	81	fb	71	72	b0	62	47	6c
bd	0e	bd	3f	be	54	2f	c9	ec	51	16	5e	c3	77	44
40	3e	b6	38	7f	81	a0	50	7f	81	d3	a5	7b	7c	1f
a6	09	9f	a1	e9	62	44	d0	f8	83	28	9a	ae	be	3f
51	8c	67	51	f9	5b	3a	68	2c	37	9a	b3	1c	49	4f

1001101101101000011011000001000101111110010101010111000110000010
1100110100100000010110000111100000101101000101010000111100001001
01011101000001000000010101010110111010101101001000111100111011
00010010101001111110101111111010010001100111011001111111011

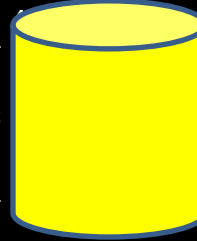
c8 01 98 2b 32 06 72 2c 12 f9 0d 1c 01 02 23
40 a5 1a d7 ec 56 02 72 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d1 19 d7 3e 1f 80
f7 ef 17 50 05 be 2f 47 7e 9 28 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 a 43 63 76 de 3c 09
6b 8d 94 4c 9 6a 2 1 03 8c 3b c3 10 67 65 ca
03 b1 25 3 2 7e 49 e4 45 67 b2 5a 54
34 97 e 1 7 c4 d1 b1 a5 1a d6 a5 67 6e ca
e f 85 ff 3c 44 2b cd d6 f8 ea f9
8f b d d 36 fd 50 81 fb 71 72 b0 62
bd e b d 3f be 54 2f c9 ec 51 16 5e c3
40 3e b6 38 7f 81 a0 50 7f 81 d3 a5
a6 09 9f a1 e9 62 44 d0 f8 83 28 9a ae
51 8c 67 51 f9 5b 3a 68 2c 37 9a b3 1c

2048 bits



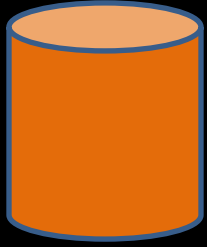
You

```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 71 05 01 02 23
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 71 05 01 02 23
1e 6f b9 85 ff 3c 44 2b cd d6 f8 71 05 01 02 23
8f bd dd d9 36 fd 50 81 fb 71 72 71 05 01 02 23
bd 6e bd 3f be 54 2f c9 ec 51 16 71 05 01 02 23
40 63 3e b6 38 7f 81 a0 50 7f 81 71 05 01 02 23
a6 09 9f a1 e9 62 44 d0 f8 83 28 71 05 01 02 23
51 8c 67 51 f9 5b 3a 68 2c 37 9a 71 05 01 02 23
```

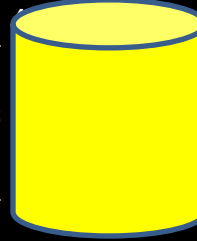


Amazon

You



```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 1f 0d 01 02 23
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 1e 6f b9 85 ff 3c 44 2b cd d6 f8
8f bd dd d9 36 fd 50 81 fb 71 72 bd 6e bd 3f be 54 2f c9 ec 51 16
40 63 3e b6 38 7f 81 a0 50 7f 81 a6 09 9f a1 e9 62 44 d0 f8 83 28
51 8c 67 51 f9 5b 3a 68 2c 37 9a
```

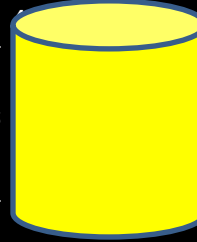


Amazon

You



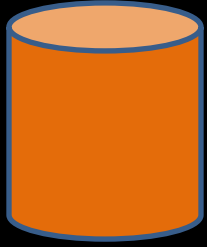
```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 7f 8d 5b 4d
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 7f 8d 5b 4d
1e 6f b9 85 ff 3c 44 2b cd d6 f8 7f 8d 5b 4d
8f bd dd d9 36 fd 50 81 fb 71 72 7f 8d 5b 4d
bd 6e bd 3f be 54 2f c9 ec 51 16 7f 8d 5b 4d
40 63 3e b6 38 7f 81 a0 50 7f 81 7f 8d 5b 4d
a6 09 9f a1 e9 62 44 d0 f8 83 28 7f 8d 5b 4d
51 8c 67 51 f9 5b 3a 68 2c 37 9a 7f 8d 5b 4d
```



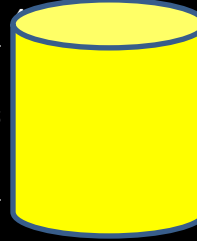
Amazon



You



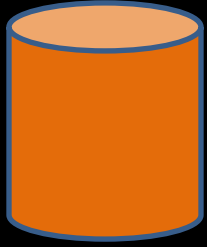
```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 1f 0d 0e 0f
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 1f 0d 0e 0f
1e 6f b9 85 ff 3c 44 2b cd d6 f8 1f 0d 0e 0f
8f bd dd d9 36 fd 50 81 fb 71 72 1f 0d 0e 0f
bd 6e bd 3f be 54 2f c9 ec 51 16 1f 0d 0e 0f
40 63 3e b6 38 7f 81 a0 50 7f 81 1f 0d 0e 0f
a6 09 9f a1 e9 62 44 d0 f8 83 28 1f 0d 0e 0f
51 8c 67 51 f9 5b 3a 68 2c 37 9a 1f 0d 0e 0f
```



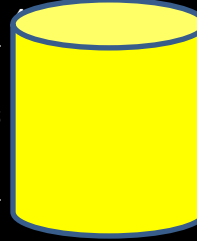
Amazon



You



```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 1f 0d 0e 0f
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 1f 0d 0e 0f
1e 6f b9 85 ff 3c 44 2b cd d6 f8 1f 0d 0e 0f
8f bd dd d9 36 fd 50 81 fb 71 72 1f 0d 0e 0f
bd 6e bd 3f be 54 2f c9 ec 51 16 1f 0d 0e 0f
40 63 3e b6 38 7f 81 a0 50 7f 81 1f 0d 0e 0f
a6 09 9f a1 e9 62 44 d0 f8 83 28 1f 0d 0e 0f
51 8c 67 51 f9 5b 3a 68 2c 37 9a 1f 0d 0e 0f
```

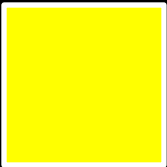
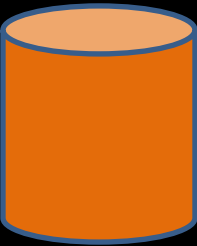


Amazon



You

Amazon



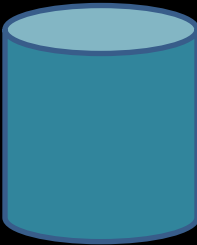
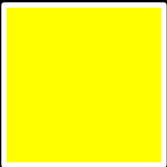
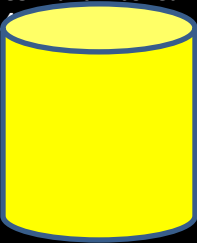
+

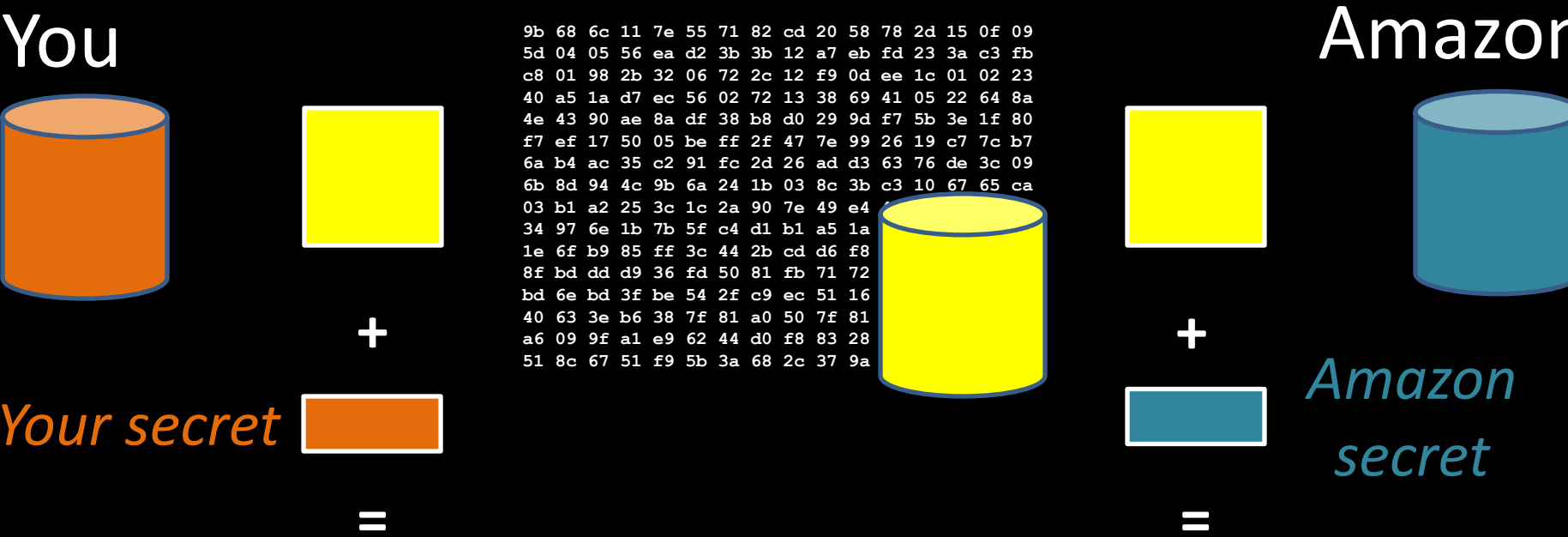
Your secret



=

```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 7d 0c 01 02 23
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a 7d 0c 01 02 23
1e 6f b9 85 ff 3c 44 2b cd d6 f8 7d 0c 01 02 23
8f bd dd d9 36 fd 50 81 fb 71 72 7d 0c 01 02 23
bd 6e bd 3f be 54 2f c9 ec 51 16 7d 0c 01 02 23
40 63 3e b6 38 7f 81 a0 50 7f 81 7d 0c 01 02 23
a6 09 9f a1 e9 62 44 d0 f8 83 28 7d 0c 01 02 23
51 8c 67 51 f9 5b 3a 68 2c 37 9a 7d 0c 01 02 23
```





You



+

Your secret



=



```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 45 67 b2 5a 54
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a d6 a5 67 6e ca
1e 6f b9 85 ff 3c 44 2b cd d6 f8 ea f9 d3 46 de
8f bd dd d9 36 fd 50 81 fb 71 72 b0 62 47 6c 91
bd 6e bd 3f be 54 2f c9 ec 51 16 5e c3 77 44 a3
40 63 3e b6 38 7f 81 a0 50 7f 81 d3 a5 7b 7c 1f
a6 09 9f a1 e9 62 44 d0 f8 83 28 9a ae be 3f 03
51 8c 67 51 f9 5b 3a 68 2c 37 9a b3 1c 49 4f 9b
```

Amazon



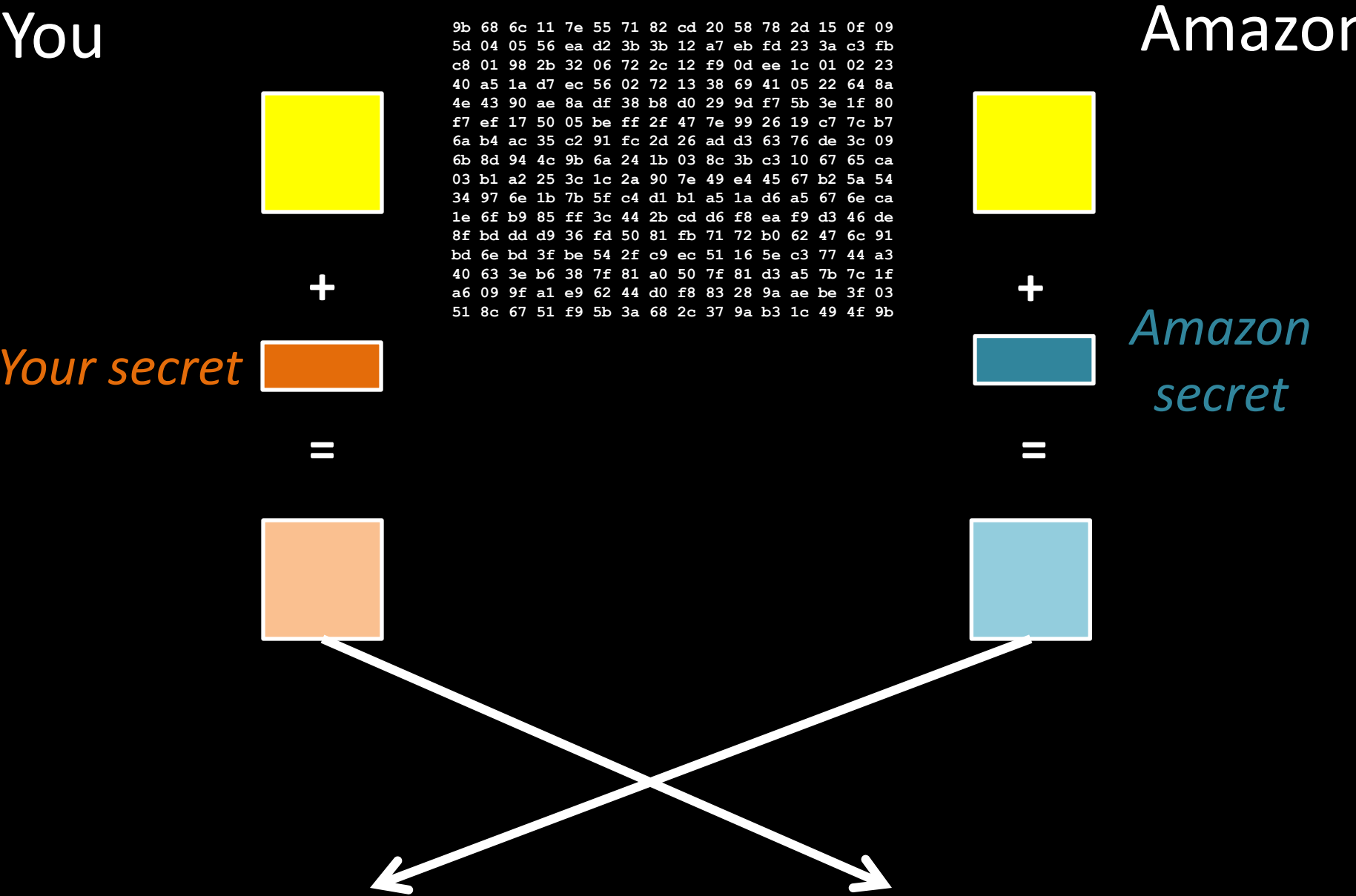
+

*Amazon
secret*



=





You



Amazon

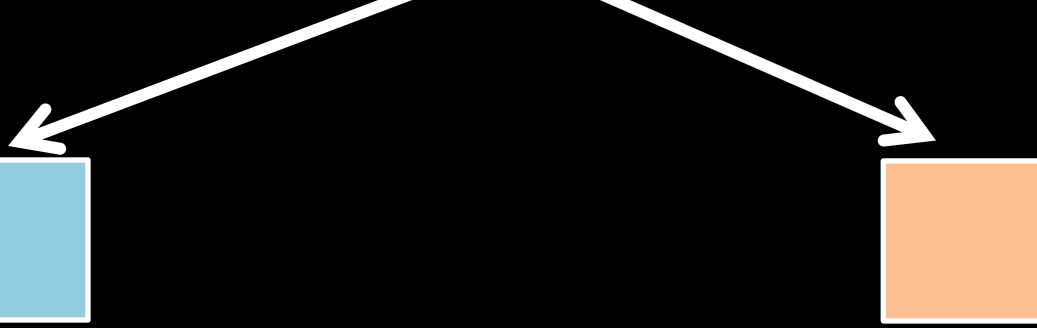
You

Amazon



+

Your secret



You

Amazon



+

+

Your secret



*Amazon
secret*



You

Amazon



+

+

Your secret



*CS 105
secret*

=

=



Shared secret

You

Amazon



+

+

Your secret



*CS 105
secret*

=

=



Shared secret



```
6c 2c 2b e1 98 9f 5d e7 d5 c6 bb 7c 51 f5 d4 69
84 fb 9d 9b 27 2b d3 ef aa 38 31 34 e9 e1 89 7c
5f 71 0a d1 2e 37 d9 5e f2 38 48 77 f7 ee 3f 57
8d a5 9a e8 d2 22 46 f6 31 6a 2f c8 39 d5 cc b5
e7 12 99 4b 32 bf 74 b9 55 fd f5 08 87 6e ea 6e
66 df 0b 19 f4 d9 25 eb 66 2a 64 10 ac 1a 3e d7
4b 98 67 d6 43 90 56 42 e4 e9 c3 d1 fa 16 49 f0
31 3e ff 1f 82 f6 2c de ba 25 f3 97 9b cd 8d 7c
bd ac 8f 95 77 11 19 04 66 87 74 74 4f 7d b1 f7
f8 2a a7 fc de 97 df 54 3a d7 4a dd eb 13 3a 45
9d b7 ad e2 f5 7b b9 fb d6 45 d1 82 61 03 8b 13
0f da 1c 5a 63 80 cd 5b af eb b1 ed a0 b4 19 fa
7b a5 07 84 46 e0 33 23 08 0e 06 af f5 15 55 7f
38 a2 16 71 06 c9 f6 a6 01 72 9a 6a 2e 7b b0 d1
ed a6 e6 37 6e 0e b8 bf 81 a9 22 83 61 5e 60 84
fd 44 4e 99 0b d2 bf 82 96 d9 a4 71 9d 4b 72 5c
```

XOR

0 XOR 0 → 0

0 XOR 1 → 1

1 XOR 0 → 1

1 XOR 1 → 0

XOR

0 ← 0 XOR 0

0 XOR 1 → 1

1 XOR 0 → 1

1 XOR 1 → 0

XOR

0 ← 0 XOR 0

0 ← 1 XOR 1

1 XOR 0 → 1

1 XOR 1 → 0

XOR

0 ← 0 XOR 0

0 ← 1 XOR 1

1 ← 0 XOR 1

1 XOR 1 → 0

XOR

0 ← 0 XOR 0

0 ← 1 XOR 1

1 ← 0 XOR 1

1 ← 1 XOR 0

Message: 00101001010

Key: 10101011011

Encrypted: 1

Message: 00101001010

Key: 10101011011

Encrypted: 01

Message: 00101001010

Key: 10101011011

Encrypted: 001

Message: 00101001010

Key: 10101011011

Encrypted: 0001

Message: 00101001010

Key: 10101011011

Encrypted: 10001

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message:

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 0

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 10

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 010

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 1010

Exclusive OR (XOR)

Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 00101001010

You



+

Your secret



=



Amazon



+

*Amazon
secret*



=



Shared secret

Attacker

You



+

Your secret

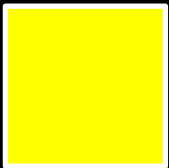


=



Shared secret

Attacker



Amazon



+

*Amazon
secret*



=



You



+

Your secret



=



Amazon



+

*Amazon
secret*

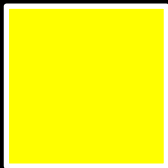


=



Shared secret

Attacker



+



+



You



+

Your secret



=



Amazon



+

*Amazon
secret*

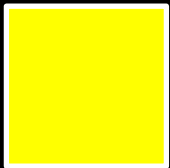


=



Shared secret

Attacker



+



+



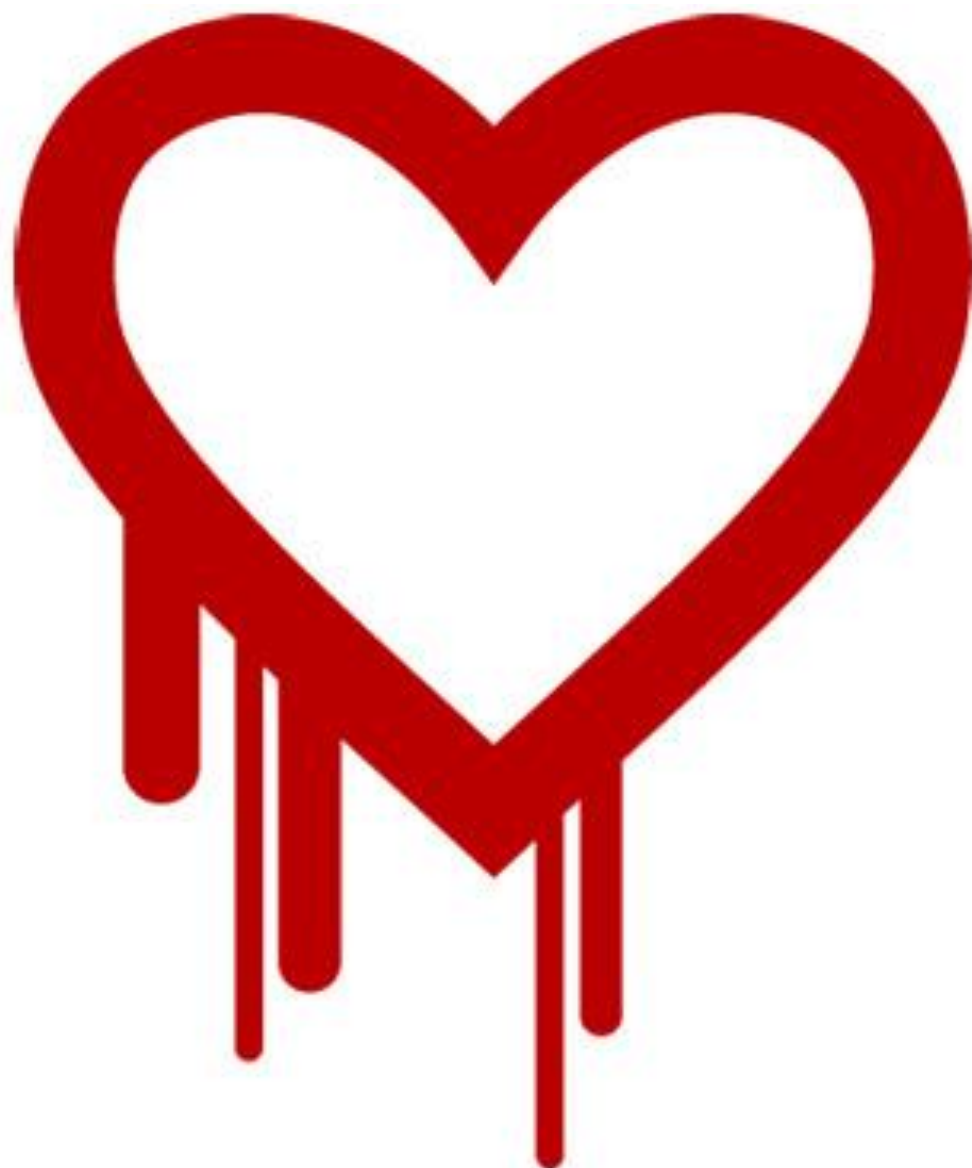
=



You

Amazon





You

Amazon

```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 45 67 b2 5a 54
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a d6 a5 67 6e ca
1e 6f b9 85 ff 3c 44 2b cd d6 f8 ea f9 d3 46 de
8f bd dd d9 36 fd 50 81 fb 71 72 b0 62 47 6c 91
bd 6e bd 3f be 54 2f c9 ec 51 16 5e c3 77 44 a3
40 63 3e b6 38 7f 81 a0 50 7f 81 d3 a5 7b 7c 1f
a6 09 9f a1 e9 62 44 d0 f8 83 28 9a ae be 3f 03
51 8c 67 51 f9 5b 3a 68 2c 37 9a b3 1c 49 4f 9b
```



+



=



+

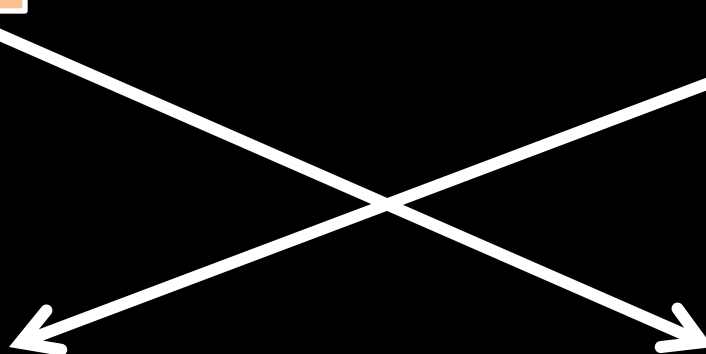


=



Your secret

*CS 105
secret*



You

Amazon

```
9b 68 6c 11 7e 55 71 82 cd 20 58 78 2d 15 0f 09
5d 04 05 56 ea d2 3b 3b 12 a7 eb fd 23 3a c3 fb
c8 01 98 2b 32 06 72 2c 12 f9 0d ee 1c 01 02 23
40 a5 1a d7 ec 56 02 72 13 38 69 41 05 22 64 8a
4e 43 90 ae 8a df 38 b8 d0 29 9d f7 5b 3e 1f 80
f7 ef 17 50 05 be ff 2f 47 7e 99 26 19 c7 7c b7
6a b4 ac 35 c2 91 fc 2d 26 ad d3 63 76 de 3c 09
6b 8d 94 4c 9b 6a 24 1b 03 8c 3b c3 10 67 65 ca
03 b1 a2 25 3c 1c 2a 90 7e 49 e4 45 67 b2 5a 54
34 97 6e 1b 7b 5f c4 d1 b1 a5 1a d6 a5 67 6e ca
1e 6f b9 85 ff 3c 44 2b cd d6 f8 ea f9 d3 46 de
8f bd dd d9 36 fd 50 81 fb 71 72 b0 62 47 6c 91
bd 6e bd 3f be 54 2f c9 ec 51 16 5e c3 77 44 a3
40 63 3e b6 38 7f 81 a0 50 7f 81 d3 a5 7b 7c 1f
a6 09 9f a1 e9 62 44 d0 f8 83 28 9a ae be 3f 03
51 8c 67 51 f9 5b 3a 68 2c 37 9a b3 1c 49 4f 9b
```



+

Your secret



=

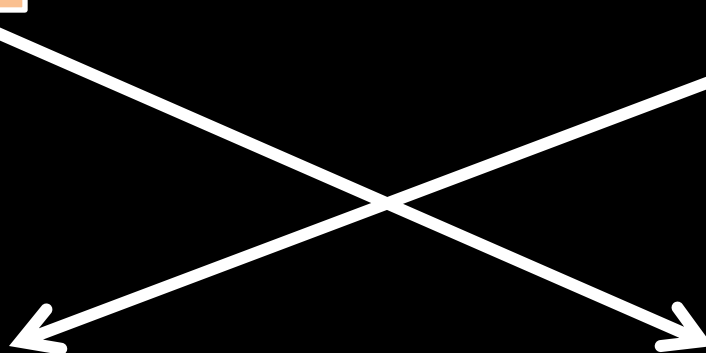


+



=

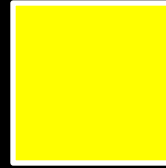
*Amazon
secret*



You

Amazon

Attacker



You

Amazon

Attacker



Message: 00101001010

Key: 10101011011

Encrypted: 10000010001

Encrypted: 10000010001

Key: 10101011011

Message: 00101001010