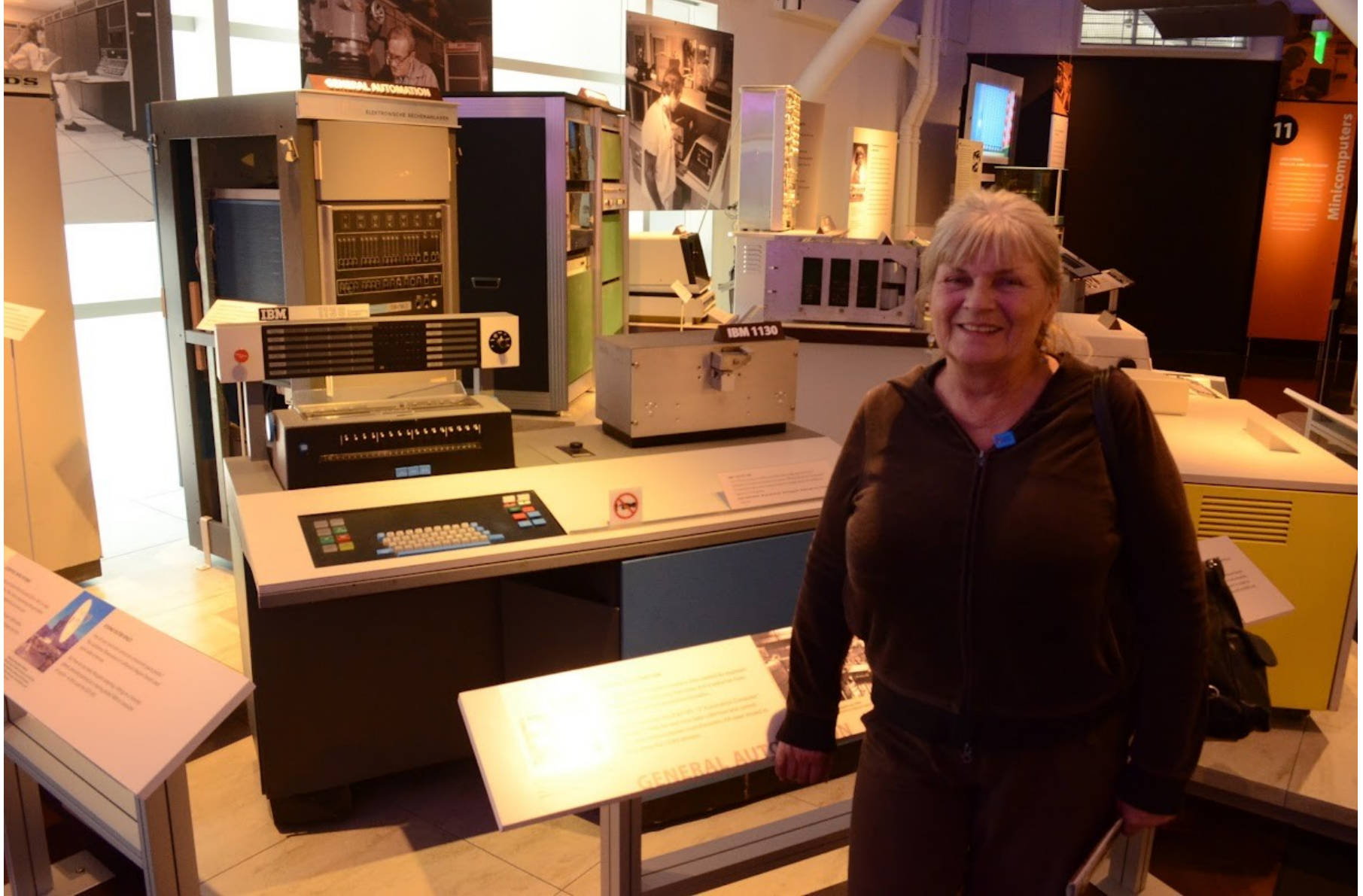
CSE 539 Course Intro

Applied Cryptography

Jed Crandall
jedimaestro@asu.edu

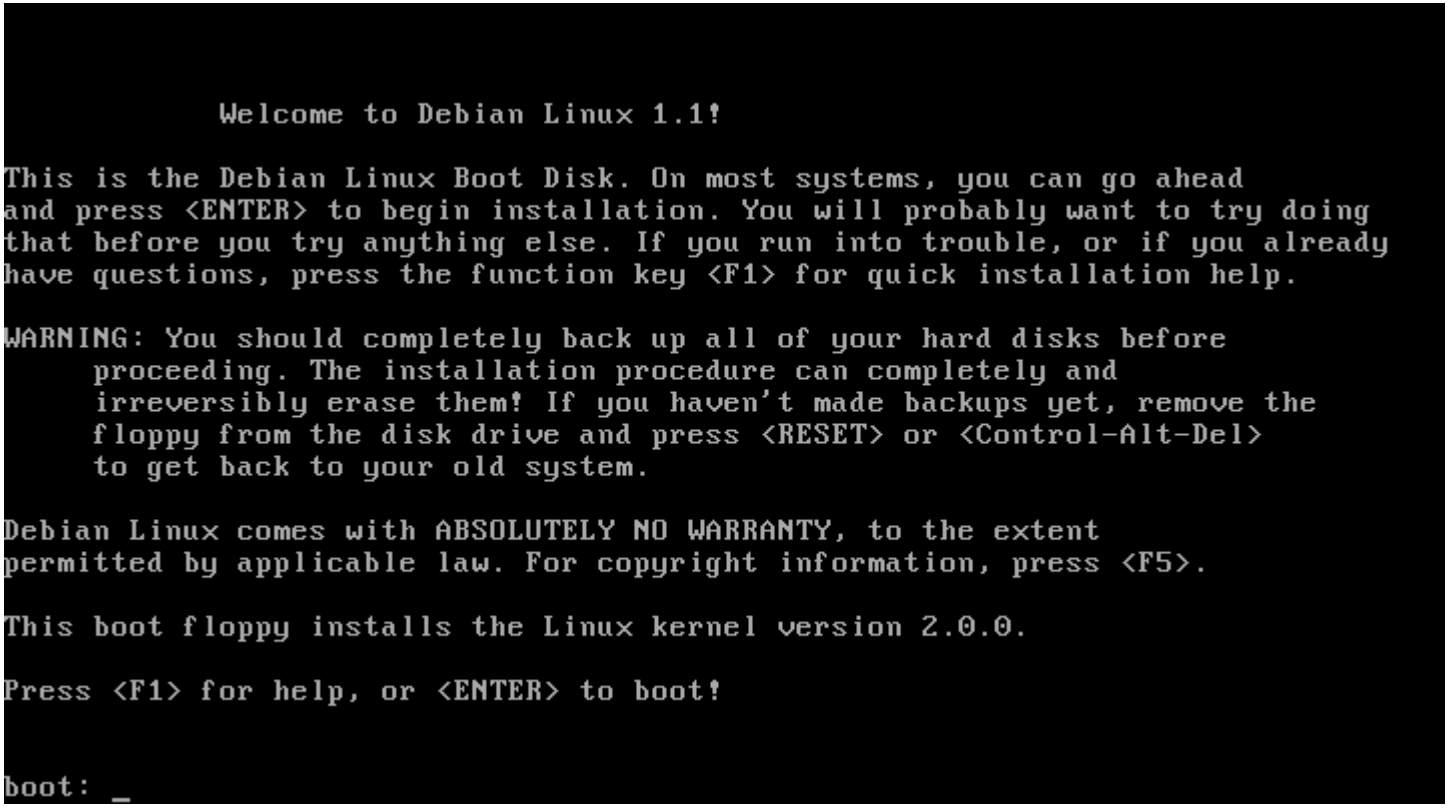
A bit about me…

- Associate Professor, SCAI *and* Biodesign Center for Biocomputation, Security, and Society
- Research is about Internet Freedom, including:
  - Internet censorship and censorship evasion
  - Machine-in-the-middle attacks, adversarial networking
  - Privacy, forensics, and a few other things


IBM
IBM 1130
11
Minicomputers

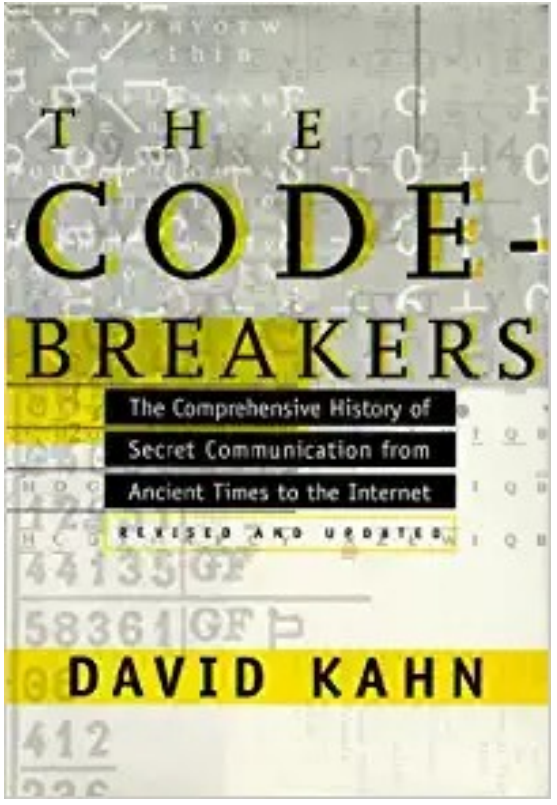

IBM
1130
IBM
GENERAL AUTOMATION
Not every minicomputer company was created by engineers
jumping ship. A marketing executive and a sales
Honeywell founded General A

https://commons.wikimedia.org/wiki/File:Apple_II_typical_configuration_1977.png



https://archive.org/details/debian_1.1

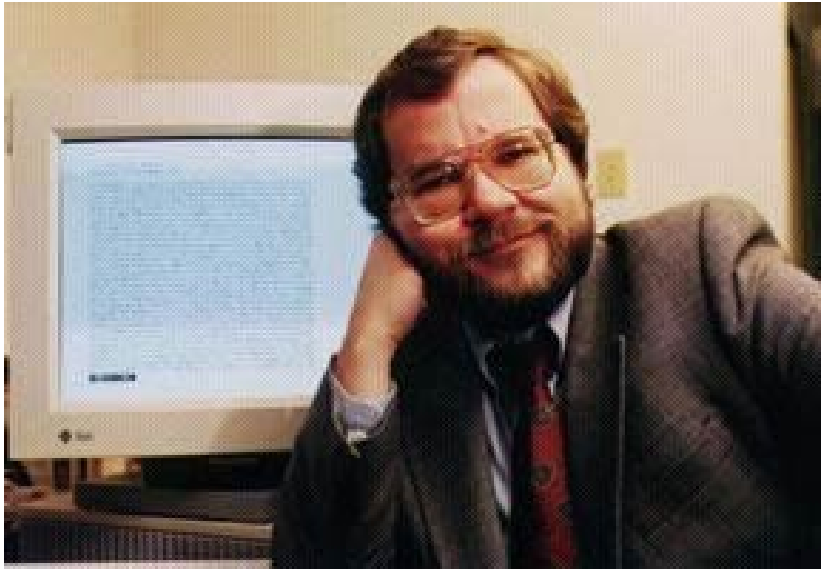
5-minute history of crypto...



https://en.wikipedia.org/wiki/Voynich_manuscript#/media/File:Voynich_Manuscript_(32).jpg

https://en.wikipedia.org/wiki/Enigma_machine#/media/File:Enigma_(crittografia)_-_Museo_scienza_e_tecnologia_Milano.jpg

https://www.cryptomuseum.com/crypto/usa/cvas/index.htm



https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

This semester, we'll...

- Spend a lot of time on:

- Not on:

Why?

- The Signal protocol covers all the basics (hash functions, symmetric crypto, asymmetric crypto, authentication, *etc.*), things that are important to privacy (deniable encryption, perfect forward secrecy, double ratchet, zero-knowledge proofs, *etc.*), and touches on other subjects (*e.g.*, blockchain).
- Closer to my research area than bitcoin.

I’m not a crypto researcher, but my research touches on crypto from time to time...

THE CITIZEN LAB

Let C be the RSA encryption of 128-bit AES key k with RSA public key (n, e). Thus, we have

$$C \equiv k^e \pmod{n}$$

Now let C_b be the RSA encryption of the AES key

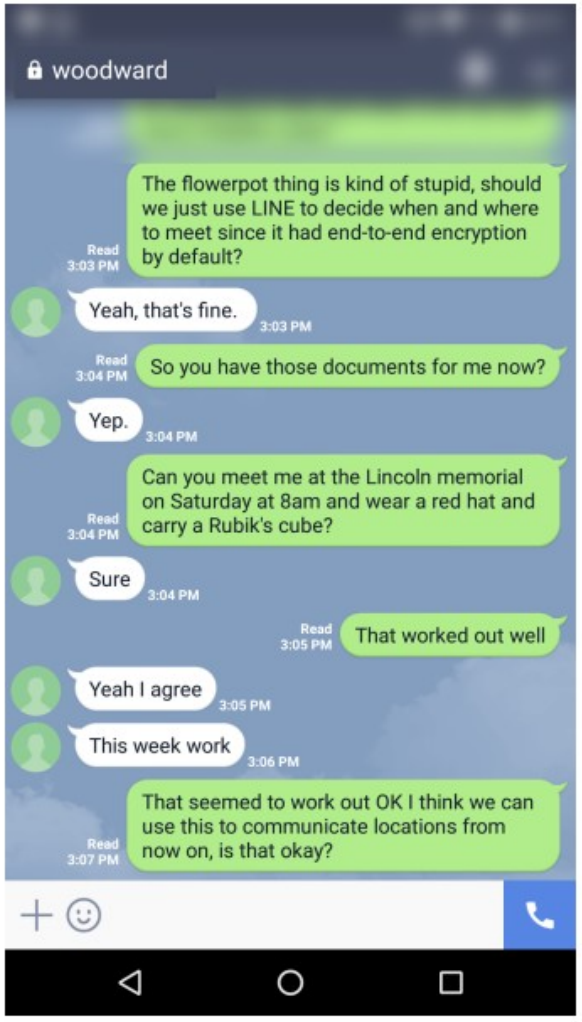
$$k_b = 2^b k$$

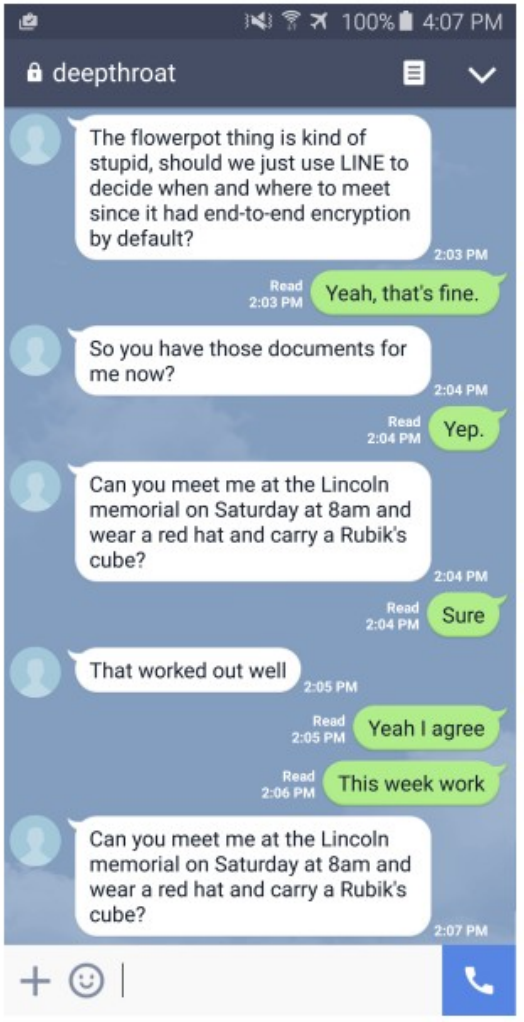
i.e., k bitshifted to the left by b bits. Thus, we have

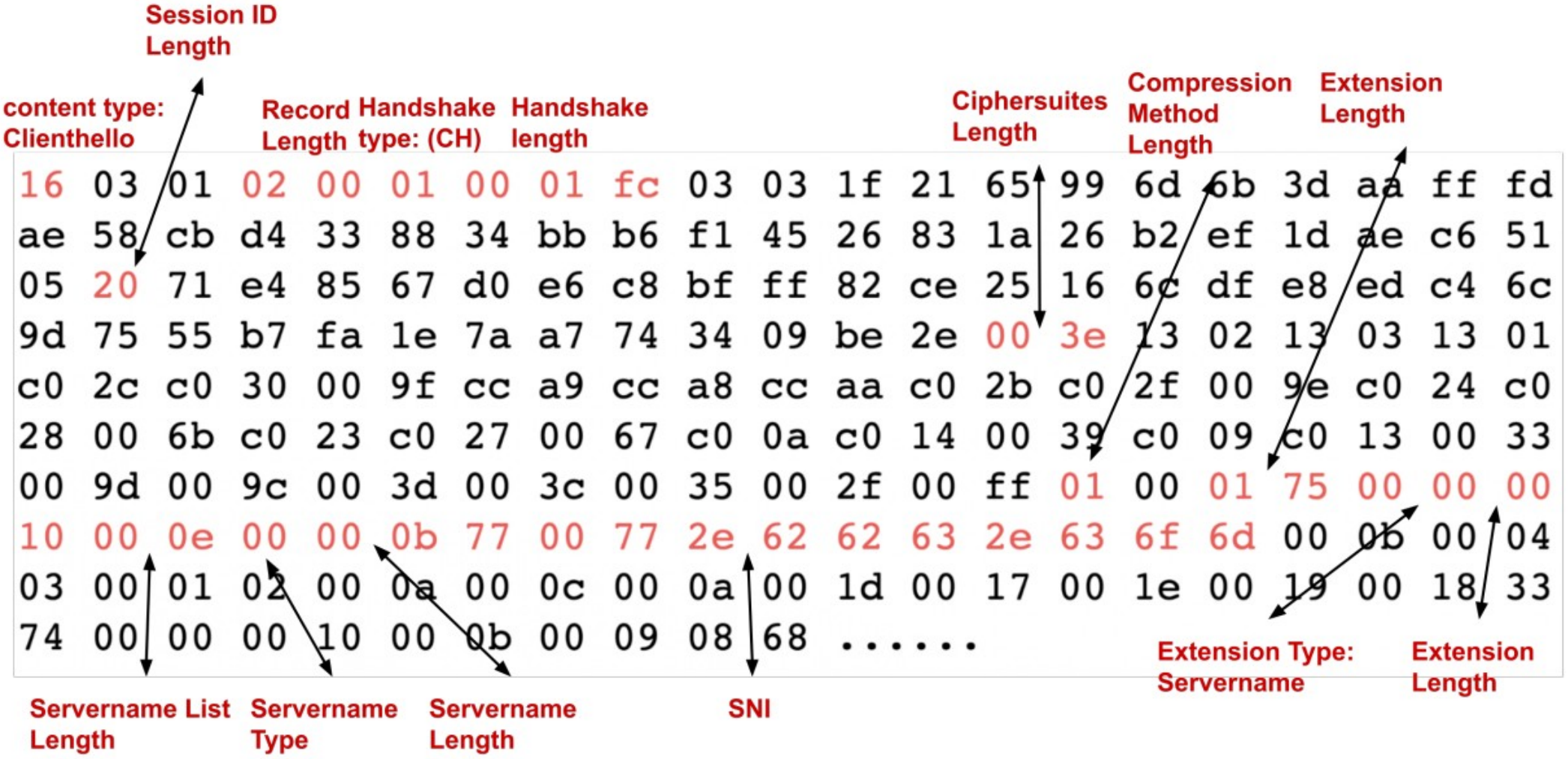
$$C_b \equiv {k_b}^e \pmod{n}$$

We can compute C_b from only C and the public key, as

$$\begin{aligned} C_b &\equiv C(2^{be} \bmod n) \pmod{n} \\ &\equiv (k^e \bmod n)(2^{be} \bmod n) \pmod{n} \\ &\equiv k^e 2^{be} \pmod{n} \\ &\equiv (2^b k)^e \pmod{n} \\ &\equiv {k_b}^e \pmod{n} \end{aligned}$$


woodward
The flowerpot thing is kind of stupid, should we just use LINE to decide when and where to meet since it had end-to-end encryption by default?
Read 3:03 PM
Yeah, that's fine.
3:03 PM
So you have those documents for me now?
Read 3:04 PM
Yep.
3:04 PM
Can you meet me at the Lincoln memorial on Saturday at 8am and wear a red hat and carry a Rubik's cube?
Read 3:04 PM
Sure
3:04 PM
That worked out well
Read 3:05 PM
Yeah I agree
3:05 PM
This week work
3:06 PM
That seemed to work out OK I think we can use this to communicate locations from now on, is that okay?
Read 3:07 PM


100% 4:07 PM
deepthroat
The flowerpot thing is kind of stupid, should we just use LINE to decide when and where to meet since it had end-to-end encryption by default?
2:03 PM
Read 2:03 PM
Yeah, that's fine.
So you have those documents for me now?
2:04 PM
Read 2:04 PM
Yep.
Can you meet me at the Lincoln memorial on Saturday at 8am and wear a red hat and carry a Rubik's cube?
2:04 PM
Read 2:04 PM
Sure
That worked out well
2:05 PM
Read 2:05 PM
Yeah I agree
Read 2:06 PM
This week work
Can you meet me at the Lincoln memorial on Saturday at 8am and wear a red hat and carry a Rubik's cube?
2:07 PM


Session ID Length
content type: Clienthello
Record Length
Handshake type: (CH)
Handshake length
Ciphersuites Length
Compression Method Length
Extension Length
16 03 01 02 00 01 00 01 fc 03 03 1f 21 65 99 6d 6b 3d aa ff fd
ae 58 cb d4 33 88 34 bb b6 f1 45 26 83 1a 26 b2 ef 1d ae c6 51
05 20 71 e4 85 67 d0 e6 c8 bf ff 82 ce 25 16 6c df e8 ed c4 6c
9d 75 55 b7 fa 1e 7a a7 74 34 09 be 2e 00 3e 13 02 13 03 13 01
c0 2c c0 30 00 9f cc a9 cc a8 cc aa c0 2b c0 2f 00 9e c0 24 c0
28 00 6b c0 23 c0 27 00 67 c0 0a c0 14 00 39 c0 09 c0 13 00 33
00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 ff 01 00 01 75 00 00 00
10 00 0e 00 00 0b 77 00 77 2e 62 62 63 2e 63 6f 6d 00 0b 00 04
03 00 01 02 00 0a 00 0c 00 0a 00 1d 00 17 00 1e 00 19 00 18 33
74 00 00 00 10 00 0b 00 09 08 68 ......
Servername List Length
Servername Type
Servername Length
SNI
Extension Type: Servername
Extension Length

Syllabus...

RED TEAMING.
PENETRATION TESTING.
OFFENSIVE SECURITY.

DEVILSEC

https://discord.io/DevilSec