- Authenticaton
  - Paper key exchange
    - Prepend to string -> so mck
    - Everything (end to end) that is
  - OTP withnostic allience
msg

I did not send that

more can first meet

someone who can verify

use "Mac"

do not use "iPad"

- Deborah
Perfect Forward Secrecy - ephemeral key - key cannot be reused - long term secret
Correct key
Look at box, choose answer all but the
such
No, my

puts yes/

B/c

Socialist Alliance (single explanation)
- has a shared secret
- same for both.
- if secret leaks, no msgs can be exposed.
Step 1: use DH to exchange a key.

Is often done via AKE/SIGMA.

Authenticated key exchange

Pub keys & Diffie-Hellman

Signature MAC

Suffer from MiTM
Send to Bob

Compute $q_1, q_2, q_3$

Alice picks $a_1, a_2, a_3$

$h = y^x \mod n$

Thus secret $x$, Bob has secret $y$, check

Suggest new $y$ in description
- Send to Alice
- Compute $p = \overline{p}_0 = q_3$, $q_6 = q_7$  
- Pick random $u$  
- Compute $q_2^u = q_{2u}$  
- Compute $q_3 = q_{3u}$  
- Pick $b_2, b_3$  
- Compute $q_{2b}$  
- $p_b$
Compute \( R^2 = (\frac{19}{86})^2 \)

Compute \( p = 4 \), \( q = \frac{9}{16} \)

Compute \( p = 4 \), \( q = \frac{9}{16} \)

Second round

Randomness

Randomness

If no win after 4 rounds, \( p = 4 \), \( q = \frac{9}{16} \)

Randomness

Randomness

Randomness

Alice's deco
After receiving $f_a, g_a = f_a$,

Send Alice $R_b$

Check if $g_a = f_a$?

Compute $R_b = (R_a - 6)^3$

Compute $g_b = (g_a^6)^3$

Yes

No
\[ e_q e_{23} = (g, r) \quad \text{where} \quad h = \frac{s}{x - y} \]

\[ = (g, -r) \quad \text{for} \quad x \neq y \]

\[ e_{q_3} e_{23} e_q = (g, 1) \]

\[ = (q_1, q_2) e_{23} e_q = (g, 1) \]

\[ \frac{q_1}{q_2} \]

\[ r_{ab} = \frac{r_a}{r_b} \]
Good morning, everyone.

To 82.5 vs do you guys say on the answer.

I think we should have a sense of the answer.

Let's come up with some answers to some of these questions.

Randomized Response Technique.
Let's go and come back later.

So yes, yes — no body chance.