- Known Plaintext

- Chosen Plaintext

- Chosen Ciphertext

Cryptography is a broad topic!
Chosen plaintext

- chosen key - not the actual key but the relationship between 2 keys.
2. Use a unit conversion percent

- Consistent linear measure

- Linear vs. Planar
Weedness vs. Shoots w/ nit in PES.

Lesser Chrysin in control
Lesser Chrysin + Diff.

Adapt fixed Chrysin in plant text.
Compute $C_{g(x)}$ and $g(x)$.

Then, pick a random seed $y$.

Alice picks $x$. Public: $C_{g(x)}$.

Bob picks $y$. Public: $C_{g(x)}$.

First public key: $C_{g(x)}$. (Key exchange)

Then, $x = 1976$.
\[
\begin{align*}
\text{Case } 4: & \quad q_0 = 1, q_1 = 3, q_2 = 4, q_3 = 2, q_4 = 1, q_5 = 3, q_6 = 4 \\
\text{If } n = 5 \quad q_0 \neq q_4 \quad \text{not 4}
\end{align*}
\]
Diffie–Hellman works?

- that is only Alice & Bob know the key?

\[ \rightarrow \text{unknown.} \]

\[ \rightarrow \text{equiv to solving the "discrete logarithm problem over finite fields".} \]
Let numbers.

Compute: $\log_b c \equiv p = \log_b a$.

Either: $n \equiv 3$ (mod 7)
- with pulse info only

- Date: 4 8 (use other method)

- Bug done with satisfactory

- Feedback: 4 8

- Provide more details

Diff: 4 8
\[ n = p \times q \] 

If \( p \) and \( q \) are prime numbers.

\[ \text{RSA} = \text{Public Key Encryption} \]

Public Key step...
\[ \overline{e} = \overline{d(\text{mod}\ n)} = 1 \]

Find such that

\[ G(n) \]

Select e to be relatively prime to 65537.

\[ \phi(n) = (p-1)(q-1) \]
\[ \text{object}_e \in [M_{9d}] \quad \text{median} \quad m = M \]

(9, m) = prime key

(2, n) = public key

detect forever

\[ n \times a \neq \text{even}, \ e \]
\[ n = \frac{1024 \text{ bit}}{2^{16}} \]

Time taken \( \ll \) 2^n but face to

but face = preference in
Pub Key can do key escrow / authentication

Alice

Bob

[pub, priv]

bytes

$p(k)$(key)

key escrow / authentication
Alex

Password

I can't remember it.

Please ask the manager. (Password)

Further instructions:

Ω
\text{new}\leftarrow F_{\text{new}}^G(r)

\text{Alice}\leftarrow \text{Bob}\quad \text{Bob}\leftarrow \text{Alice}

\text{challenge message} \rightarrow \text{response message}

\text{challenge needs nonce secret}