- Browser
- Applications
- OS
- Certificate Store (pub key & sign, etc.)
- Root of Trust
1984 "Reflection on Trusting Trust"

Ken Thompson
Pam Sylvestre

1983 / 1984

Turning Around Leadership
-> Logs in as root
- Root user 
- "Super User"
- User
The Unix Backdoor
Log in Progress

Drug best = just passed

Later

Shell

arrow
No

Check (string, short)

get string

print password

get string

print user

log in
For broader
ask broad

Bob cc

else

if begin

else check this invalid problem

Check for compatibility

 gallons
If conditions described

| Functionality: str, to Bridge U

# Generation: use in Broken to be

L. Defined a C - completed

Bad CC version 2
detail before - cc-12 source forecast

(simplified)

(a) get Board cc-12 - bu - cc

Compare cc with Board cc-12 - bu

← get Board cc-12 with Board cc-12

Compare Board cc-12 with Board cc-12
Build x Repeat

- Just do it

How do we best software?
Find \( p \sim 1 \mod n \).

\[
\text{Choose } e \in (65537, \phi(p^1(q^{-1})) = (p-1)(q-1))\ \\
\begin{align*}
\phi(n) &= \phi(p q) \\
&= \phi(p) \phi(q) \\
&= (p-1)(q-1) \\
&= n - 1 \\
&= \Phi \cdot q
\end{align*}
\]

why? why? why?

- 2 prime, \( p \neq q \) -
- \( \Phi \), \( \frac{n}{\Phi} \) -
- \( n \) -
- \( n \) -

RSA - need 2 keys

how? how?
\[ m = n \pmod{p} \quad \text{or} \quad m = n \pmod{p} \]

\[ m = n \pmod{p} \]

\[ x < \underbrace{m \pmod{n}}_{\text{message}} \]
\[ n \in \mathbb{Z}^+ = \{ 0, 1, 2, \ldots, n-1 \} \]
\[ p = 3, \quad q = 5, \quad n = 15 \]

\[ \mathbb{Z}_q^n = \{1, 2, 4, 7, 8, 11, 13, 14\} \]

\[ 2^m = \{1, 2, 4, 8, 11, 13, 14\} \]

\[ 2^m = \{1, 2, 4, 8\} \]
\[ (p-1) (g-1) = \phi(n) \]

\[ p \equiv 2 \pmod{3} \]

\[ 1 = \frac{1}{\phi(n)} \]

\[ n = p \times q \]

What numbers are in \( Z_n \) but not in \( Z^*_n \)?
do not share prime with n

\[ ab = an + pq \] (\text{i.e., all mod } n = 1) \]

and does not share any prime with n

\[ a, b \in \mathbb{Z}^* \]

\[ \text{if } a, b \in \mathbb{Z}^* \]

\[ \text{a is closed under multiplicative.} \]
Closed

( at most n)

\[ x \in \mathbb{Z}_n \]

\[ \Rightarrow \]

\[ y \in \mathbb{Z}_n \]

Y \leftarrow \text{no such prime with } y
Show $S_n = \sum_1^n$ 

\[ S = \{a_1, a_2, \ldots, a_n \} \]

Let \( n \in \mathbb{Z}^+ \)

\[ Z_n = \{6a, 6b, 6c, 6d \} \]