SPN ciphers -

Substitution permutation Network

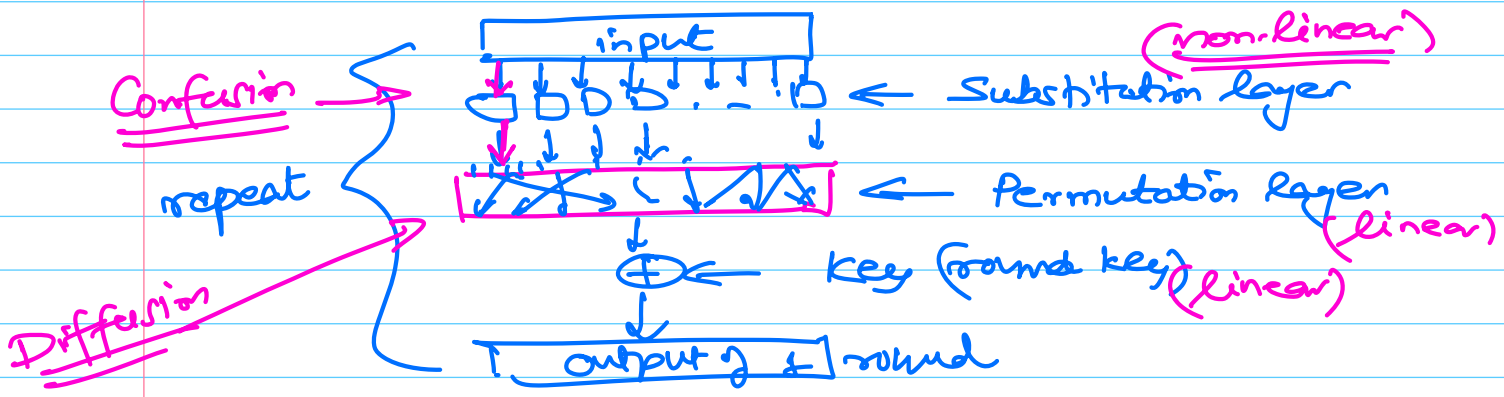
AES design document

— NIST

for ref.

13-02-2025

SPN structure:



'if a cryptosystem is linear Then it is easy to break. → $C = Ax + k$

$= [A'][x\ 1]$

Gaussian elimination → solve for A'.

Ref. → Hill cipher

Avalanche effect — a small input change causes drastic change in the output

(Caused by combination of Subs. & Perm. layers)

AES- a very strong block cipher
Has withstood the test of time

So far- **Confidentiality**

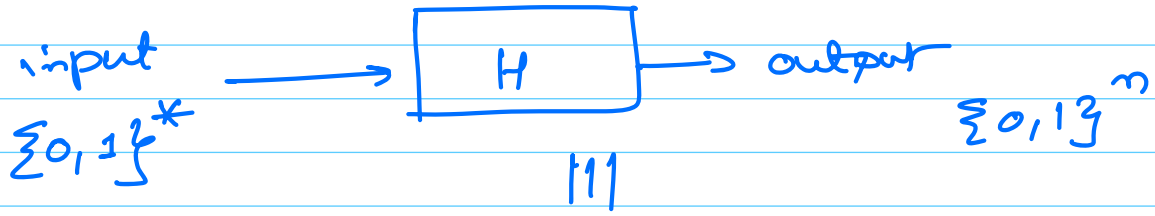
↳ achieved using encryption

Integrity : data is not modified in transit

Today's class: a cryptographic object which does not have a secret key & yet has some security guarantees

Object:

Hash function

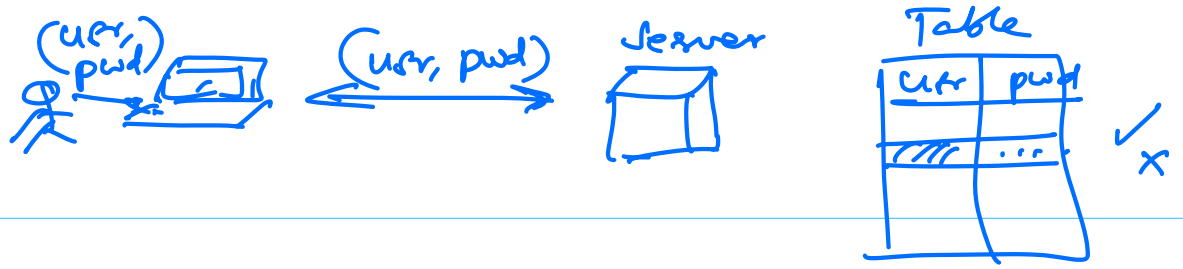


Random Oracle:

pick a random x, y : $\Pr[f(x) = y] = \frac{1}{2^n}$

① **Use-case 1:**

Password security



A very bad idea

Why?

data breach → devastating

Store the passwords as —

hash (pwd)

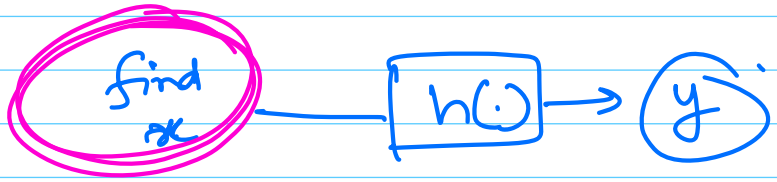
usr	h(pwd)
⋮	⋮

if someone knows h(pwd), it is computationally hard to find pwd.

Preimage resistance:

given h(x) it is computationally hard to find x

Generic attack:

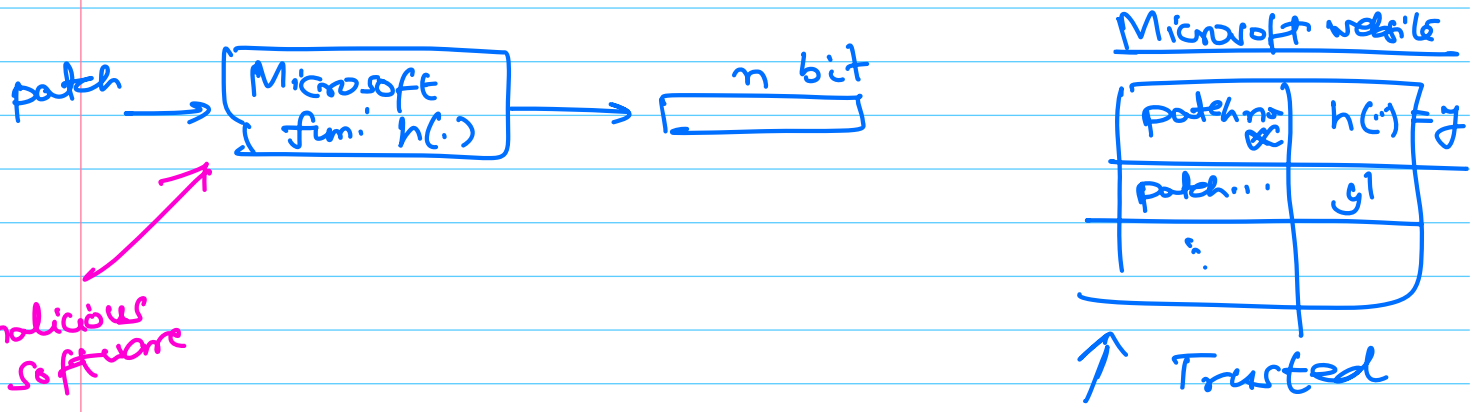


y is known

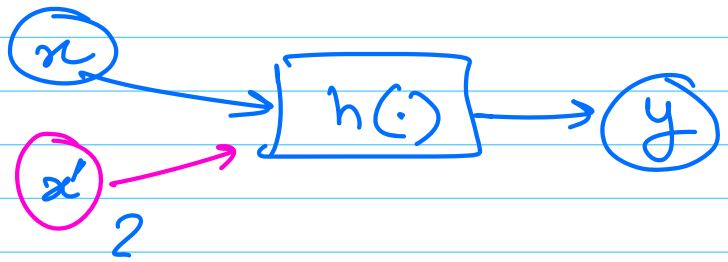
effort = 2^n

② Use-case no. 2

Software download



No one should be able to create a malicious software which has the same hash value as the original patch.



$x \neq x'$

Second Preimage attack:
Given (x, y), it should be computationally hard to find an x' s.t $h(x') = y$

Generic attack:

input $x \longrightarrow h(x) = y$

give y to preimage attacker
— success in $\geq 2^n$ trials

2^{nd} preimage in $(2^n + 1)$ trials

③ Use-case 3:

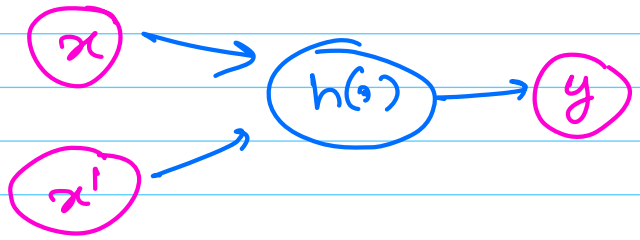
Co-development of software

- we want to check if contents of the file got modified

Small digest of the document

Collision resistance:

$x \neq x'$



It is computationally hard to find two diff. inputs which have the same output.

Collision attacker $\leq$ Second preimage attacker

Jan	
feb	18
Mar	5
Apr	
May	13, 5, 25, 27
June	27, 7, 23

July.	11, 3
Aug	- 13, 23, 12, 19
Sep	- 9, 6, 17, 29, 1, 6, 27, 16, 15
Oct	- 17, 2, 21, 12
Nov	- 3, 18,
Dec	- 29, 27 (13, 13)

Collisions happen with high pr. in about $2^{n/2}$ trials.

$x \longrightarrow h(x)$ $\quad$ $h(\cdot)$ is a random oracle

$S = \{x_1, x_2, \ldots x_t\}$, N = size of output set

Pr that there is some collision in S

$$Pr(\text{collision}) = 1 - Pr(\text{no collision})$$

$$p = 1 - \left(1 \cdot \frac{N-1}{N} \cdot \frac{N-2}{N} \cdots \frac{N-t+1}{N}\right)$$

What if $t \geq 366$, Pr = 1

$$p = 1 - \prod_{i=1}^{t-1} \left(1 - \frac{i}{N}\right)$$

assume $i << N$

$$(1 - i/N) \approx e^{-i/N}$$

$$p = 1 - \prod e^{-i/N}$$

$$= 1 - e^{\frac{-1}{N}\left(\frac{(t-1)(t)}{2}\right)}$$

$$e^{-\frac{1}{2N} t(t-1)} = 1 - p$$

$$-\frac{1}{2N} \cdot t(t-1) = \ln(1-p)$$

$$\frac{1}{2N} \cdot t(t-1) = \ln\left(\frac{1}{1-p}\right)$$

$$t^2 \simeq 2N \cdot \ln\left(\frac{1}{1-p}\right)$$

$$\boxed{t \simeq \sqrt{N} \cdot \left(2 \cdot \ln \frac{1}{1-p}\right)}$$

const

for $N = 365$

$p = 1/2$ $t = 23$

$p = 0.75$ $t = \dots$

$p = 0.99$ $t = 90$

for $p = ?$

const = 1.4

Birthday paradox

(Not really a paradox, but a counter-intuitive statistical fact)