Name :- Darpan Gaur   Assignment - 2

Roll No :- CO21BTECH11004   CS6160

DATE: / /
PAGE:

Que 1 p, q be primes such that q divides p-1. $g^q = 1$.

We know algorithm A $\Rightarrow$ given g^{α} finds $g^{1/\alpha} \bmod p$

Also we know g^{α}, g^{β}. Find $g^{\alpha\beta}$.

Sol^n Assumption :- We know g.

We can find $g^{1+\alpha} = g \cdot g^{\alpha}$ — (1)

$g^{1+\beta} = g \cdot g^{\beta}$ — (2)

Also, $g^{\frac{1}{1+\alpha}}$ & $g^{\frac{1}{1+\beta}}$ — (3) by using A on $g^{1+\alpha}$ & $g^{1+\beta}$

$$g^{1+\alpha} \cdot g^{1+\beta} = g^{2+\alpha+\beta} \quad \text{— (4)}$$

Now, $g^{\frac{1}{1+\alpha}} \cdot g^{\frac{1}{1+\beta}} = g^{\frac{1+\beta+1+\alpha}{1+\alpha+\beta+\alpha\beta}} = g^{\frac{2+\alpha+\beta}{1+\alpha+\beta+\alpha\beta}}$

By using A on $g^{\frac{2+\alpha+\beta}{1+\alpha+\beta+\alpha\beta}}$, we get

$$g^{\frac{1+\alpha+\beta+\alpha\beta}{2+\alpha+\beta}} = g^{\frac{(2+\alpha+\beta)+(\alpha\beta-1)}{2+\alpha+\beta}} = g \cdot g^{\frac{\alpha\beta-1}{2+\alpha+\beta}}$$

Divide by g, we get

$$g^{\frac{\alpha\beta-1}{2+\alpha+\beta}} \quad \text{— (5)}$$

From (4) we know $g^{2+\alpha+\beta}$, by using A on it we find $g^{\frac{1}{2+\alpha+\beta}}$ Multiply this by (5)

$$\Rightarrow g^{\frac{\alpha\beta-1}{2+\alpha+\beta}} \cdot g^{\frac{1}{2+\alpha+\beta}} = g^{\frac{\alpha\beta}{2+\alpha+\beta}}$$

Use A on $g^{\frac{\alpha\beta}{2+\alpha+\beta}}$ we get

$$g^{\frac{2+\alpha+\beta}{\alpha\beta}} = g^{\frac{2}{\alpha\beta}} \cdot g^{\frac{1}{\beta}} \cdot g^{\frac{1}{\alpha}}$$

DATE: / . /
PAGE:

$g^{2/\alpha\beta} \cdot g^{1/\beta} \cdot g^{1/\alpha}$

Divide by $g^{1/\alpha} \cdot g^{1/\beta}$ we get

$g^{2/\alpha\beta}$ ~~use A on~~

Use A on $g^{4\alpha\beta}$, we get

$g^{\frac{\alpha\beta}{2}}$

Now multiply $g^{\frac{\alpha\beta}{2}}$ by $g^{\alpha\beta/2}$

$\Rightarrow g^{\frac{\alpha\beta}{2}} \cdot g^{\frac{\alpha\beta}{2}} = \boxed{g^{\alpha\beta}}$

DATE: / /
PAGE:

Que 2 RSA public keys $(N_1, 3)$, $(N_2, 3)$, $(N_3, 3)$ i.e. $e=3$
with $N_1 < N_2 < N_3$
$r \in_R \mathbb{Z}^*_{N_1}$ & ciphertext $\left(r^3 \bmod N_1,\ r^3 \bmod N_2,\ r^3 \bmod N_3,\ H(r) \oplus m\right)$

~~Assuming gcd$(N_i, N_j) = 1$ for~~

Sol^n :- Let $N = N_1 N_2 N_3$. By chinese remainder theorem we can say that there exists $x < N$, such that

$x = c_1 \bmod N_1$ — ①

$x = c_2 \bmod N_2$ — ②

$x = c_3 \bmod N_3$ — ③

Now here, r^3 satisfies all above three equations.

We know that $r \in_R \mathbb{Z}^*_{N_1}$ so $r < N_1$.

As $N_1 < N_2 < N_3$ so

$r < \min(N_1, N_2, N_3)$ — ④

We can say $r^3 < N = N_1 N_2 N_3$ — ⑤

As r^3 satisfies ①, ②, ③ & ⑤

we can say that $x = r^3 \bmod (N_1 N_2 N_3)$

As we can find x and $r^3 < N_1 N_2 N_3$

so we can find r by simply taking cube root of r^3

Now, we know r.

Find $H(r)$

To find m, we find $(H(r) \oplus m) \oplus H(r)$
$= m$

So an adversary can find x, then r, then m

DATE: / /
PAGE:

Que 3 $f \to$ one-way permutation on $\{0,1\}^n$.
Public value $f^{(n)}(x)$. $f^{(0)}(x) = x$.
$M = \{1, \dots, n\}$.
For $i \in M$, $Sign(i) = f^{(n-i)}(x)$

(a) Reciever can verify the signature by computing $f^{(n)}(x)$ from $f^{(n-i)}(x)$

So Take $\underbrace{f(f.f\dots}_{i \text{ times}}(f^{(n-i)}(x))))$

By taking f i times we get $f^{(n)}(x)$
Now check this $f^{(n)}(x)$ which we obtained from $f^{(n-i)}(x)$ is equal to publically available $f^{(n)}(x)$.

If equal, then return 1
else return 0.

(b) This scheme is not one-time secure.
Say for message i, we have
$Sign(i) = f^{(n-i)}(x)$.
Now, we can find $Sign(j)$, for $j > i$ & $j \in N$
i.e, for all messages $> i$, we can find their sign using $Sign(i)$

Simply $\underbrace{f(f(f(\dots}_{j-i \text{ times}}(f^{(n-i)}(x))))) = f^{(n-j)}(x)$

Take f .. $(j-i)$ times to obtain $Sign(j)$ from $Sign(i)$.

DATE: / /
PAGE:

Que 4 ~~Q.~~ $m \in \{0,1\}^n$ is mapped ~~to~~ injectively to a subset $S_m \subseteq \{1, 2, \ldots, 2t\}$ of size k
$Sign(m) = \{x_i\}_{i \in S_m}$

(a) We must choose k such that there are ~~more~~ greater than equal to subset of size k than total number of messages

Subsets of size k = ${}^{2t}C_k$ [$2t \to$ total element to choose from]

message $= 2^n$ as $m \in \{0,1\}^n$

$$\boxed{{}^{2t}C_k \geq 2^n}$$

So we find ~~some x such that~~ minimum x in $\{0, 1, 2, \ldots 2t\}$ such that ${}^{2t}C_x \geq 2^n$

then $\boxed{k \in \{x, x+1, \ldots, 2t-x\}}$

(b) From part (a), ${}^{2t}C_k \geq 2^n$
So n is maximum when ${}^{2t}C_k$ is maximum
We know that ${}^{2t}C_k$ is maximum at $k = t$

$${}^{2t}C_t \geq 2^n$$

So $n_{max} \leq \log_2({}^{2t}C_t)$

$$\Rightarrow \boxed{n_{max} \leq \log_2\left(\frac{2t!}{t!\,t!}\right)}$$