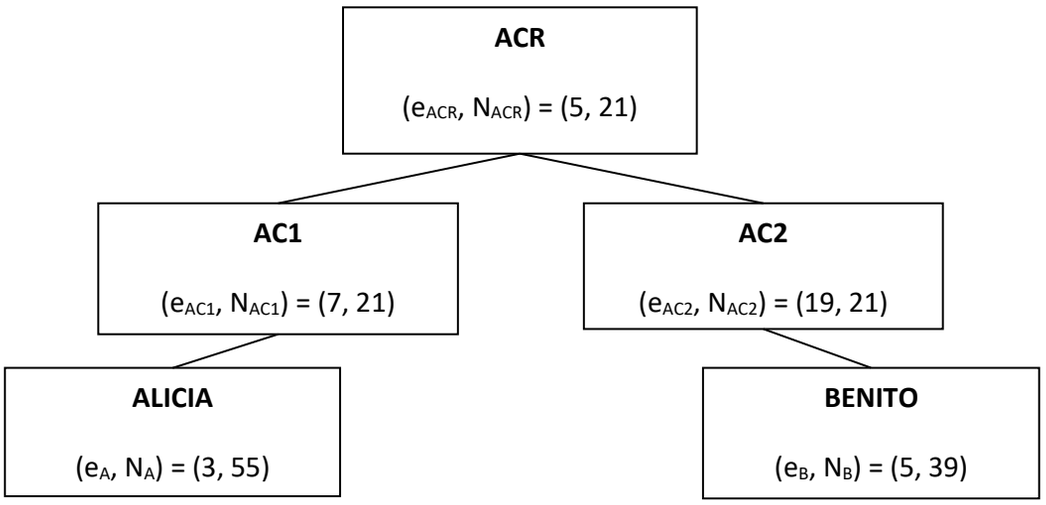
PROBLEMA 1

Alicia quiere mandar un mensaje firmado a Benito. La jerarquía de autoridades de certificación y las claves públicas y certificados en cuestión son los que se muestran en la figura a continuación.



Teniendo en cuenta las siguientes consideraciones:

- El certificado de cada entidad *i* está compuesto por su clave pública y la firma del exponente de esa clave pública por parte de la entidad emisora del certificado, es decir, $Cert_i = \{(e_i, N), F_{emisor}(e_i)\}$, siendo $F_{emisor}(e_i)$ la firma RSA realizada por la entidad emisora del certificado (entidad inmediatamente superior).
- La autoridad raíz firma su propio certificado.
- No se usan funciones resumen.
- Cada entidad posee y confía en los certificados de toda su cadena de certificación (e.g., Benito posee $Cert_{AC2}$ y $Cert_{ACR}$ y confía en ellos).

Se pide:

a) Calcule la firma RSA del mensaje M = 2 realizada por Alicia.

b) ¿Qué tendrá que enviar Alicia a Benito para que éste pueda comprobar que el mensaje fue enviado por Alicia? Justifique su respuesta.

c) Suponiendo que Alicia le envía a Benito $\{M, F_A(M), Cert_A, Cert_{AC1}, Cert_{ACR}\}$, siendo M = 2 y $F_A(M)$ el resultado calculado en el apartado a), realice TODOS los cálculos que tendría que realizar Benito para comprobar la autoría del mensaje enviado.

PROBLEMA 2

PARTE 1: ESTABLECIMIENTO DE UNA JERARQUÍA DE CERTIFICACIÓN.
Tiempo estimado: 15 min.
Puntuación máxima: 0,3 (EC) – 0,9(NO EC)

AC1: Autoridad Raíz de certificación. Genera su par de claves para la firma con *ElGamal.*

Valores:

p=2539; g =2; clave privada X_{AC1}=14; clave pública Y_{AC1}= 1150; número aleatorio para firma k=457;

AC2: Autoridad de certificación subordinada. Genera su par de claves para la firma con *RSA*.

Valores:

e_{AC2}=111; N_{AC2}= 3394;

Se pide:

a) Realizar los cálculos necesarios para que AC1 firme la clave pública de AC2 y emita así un certificado de clave pública para AC2.
El certificado tendrá el siguiente formato $cert_{AC2}$= (e_{AC2}, r, s)

b) Calcular la clave privada de AC2, asociada a su clave pública.

PARTE 2: INTERCAMBIO DE CLAVES PÚBLICAS.
Tiempo estimado: 15 min.
Puntuación máxima: 0,3 (EC) – 0,9(NO EC)

Dos usuarios, Benito y Alicia, deciden negociar mediante Diffie-Hellman una clave secreta. Para eso generan parámetros públicos y privados a partir de los siguientes parámetros globales.
Parámetros Globales: p= 719; g=3;

Alicia:

X_{ALICIA}= 16 es clave privada;
Y_{ALICIA}= 191 es clave pública;

Benito:

Y_{BENITO}= 543 es clave pública;

Se pide:

c) Realizar los cálculos necesarios para que AC2 genere un certificado de clave pública para Benito de la forma $cert_{BENITO}$= F(Y_{BENITO}), dónde F denota la firma de AC2 sobre la clave pública de Benito Y_{BENITO}.

d) Alicia recibe de Benito su certificado de clave pública. Realizar los cálculos necesarios que debe realizar Alicia para verificar el certificado de Benito siguiendo la cadena de certificación.

PARTE 3: PROTOCOLO DE DIFFIE-HELLMAN.
Tiempo estimado: 15 min.
Puntuación máxima: 0,2 (EC) – 0,6(NO EC)

Benito y Alicia intercambian sus claves públicas por un canal inseguro.

Se pide:

e) Describir los riesgos a los que se enfrentan Alicia y Benito dado que sólo Benito posee un certificado de clave pública y Alicia no cuenta con ninguna certificación. ¿Podría realizarse un ataque de *Hombre en Medio*?

f) ¿Cuál sería la clave secreta K_{AB} que Alicia y Benito negociarían, dados los datos de la parte anterior?

PARTE 4: FUNCIONES RESUMEN HMAC.
Tiempo estimado: 15 min.
Puntuación máxima: 0,2 (EC) – 0,6(NO EC)

Una vez establecida la clave de sesión (clave secreta) para las comunicaciones entre Alicia y Benito (considérese K_{AB}=7). Alicia desea enviar a Benito el mensaje M=90 (en decimal) y ambos deciden hacer uso de un código de autenticación de mensaje MAC basado en funciones resumen (HMAC). A efectos de simplificaciones, se supone 8 bits como tamaño del bloque de la función resumen. La función resumen se define como un OR entre cada uno los bloques concatenados.

Se pide:

g) Explique qué ventajas ofrece hacer uso de un código de autenticación de mensaje MAC.

h) Hallar el resultado de aplicar la HMAC sobre el mensaje.