EVALUACIÓN PARA PROPUESTAS DE TRABAJO TERMINAL

NO. DE REGISTRO DEL TT: 2020-B005

TÍTULO DEL TT: PROTOCOLO DIFFIE-HELLMAN USANDO LA CURVA ELÍPTICA PARA LA DISTRIBUCIÓN DE LLAVES DE UN CRIPTOSISTEMA SIMÉTRICO

FECHA DE EVALUACIÓN: VIERNES 4 DE DICIEMBRE DE 2020 | NO. DE VERSIÓN 1a. [X] 2a. [ ]

PREGUNTA	SI	NO	OBSERVACIONES
1. Título del TT. ¿El título corresponde al producto esperado?	X		
2. Resumen. ¿El resumen expresa claramente la propuesta del TT, su importancia y aplicación?		X	El resumen debe ser redactado de manera correcta y adecuada.
3. Palabras clave. ¿Las palabras clave han sido clasificadas adecuadamente?	X		Podrían mejorar la selección de palabras clave, sin embargo, lo dejo a criterio de los autores.
4. Introducción. ¿La presentación del problema a resolver es comprensible?		X	La introducción debe mejorarse sustancialmente.
5. Objetivo. ¿El objetivo es preciso y relevante?		X	El objetivo debe redactarse con mayor precisión, así como especificar objetivos generales y particulares.
6. Planteamiento. ¿El planteamiento del problema y la tentativa solución descrita son claros?		X	No se incluyó el planteamiento del problema, ni la motivación del proyecto.
7. Justificación. ¿Sus contribuciones o beneficios están completamente justificados? Originalidad, vinculación con población usuaria potencial, utilidad de los resultados, complejidad en su elaboración a nivel ingeniería, mejoramiento de lo existente, etc.		X	
8. Resultados o productos esperados. ¿Su viabilidad es adecuada? Tiempos, recursos humanos y materiales, alcances, costos y otros puntos que puedan impedir la culminación exitosa del trabajo.		X	
9. Metodología. ¿La propuesta metodológica es pertinente?	X		
10. Cronograma. ¿El calendario de actividades por estudiante es adecuado?	X		

DICTAMEN

APROBADO	NO APROBADO
—	X

RECOMENDACIONES DETALLADAS:

COMENTARIO 1: Aconsejo se realice una nueva redacción del resumen. La redacción presentada en esta versión 1.0 debe ser más clara. La estructura de ideas también debería ser sustancialmente mejorada. Este resumen debería presentar brevemente el proyecto identificado —al menos— el problema práctico y la propuesta de solución, con ello se permite que el lector de este documento adquiera una idea general del proyecto; lo cual considero que no se logra.

Les comparto algunos puntos sobre detalles a mejorar o corregir:

1. La redacción del resumen está en tiempo pasado, sin embargo, al ser una propuesta de proyecto es algo que no se ha realizado y, por lo tanto, no tiene sentido esta conjugación.
2. El concepto de seguridad no está definido y, con ello, no es posible entender con claridad lo que se entenderá por este.
3. Cuando se menciona “una mayor seguridad”, la palabra “mayor” hace referencia implícitamente a algo con lo que se está comparando, pero esto tampoco está expresado con claridad. Así entonces, no se entiende respecto a que se tendrá una “mayor seguridad”, suponiendo que ya se haya definido lo señalado en el punto anterior.
4. No es claro a lo que se hace referencia con “comunicaciones basadas en curva elíptica”.
5. El propósito de protocolo Diffie-Hellman no es distribuir llaves. Sugiero estudiar el protocolo para tener una noción más clara del propósito de este protocolo.
6. En el segundo enunciado del resumen, se menciona “Para lograr esto” y la palabra “esto” parece hacer referencia a la acción descrita en el enunciado anterior, es decir, “la implementación de una mayor seguridad”, sin embargo, no es claro.
7. En este mismo segundo enunciado, se refiere con “los elementos utilizados” a los recursos que permitieron la implementación referida y los cita. Sugiero evaluar si este aporta al mensaje que se desea transmitir en este resumen, esto en el sentido del primer párrafo de este comentario.

Estos son algunos puntos con el propósito de ejemplificar posibles mejoras a realizar y no debe entenderse como todo lo que se debe mejorar. Sugiero tener presente que el resumen tiene como propósito dar una descripción general del contenido del documento, en este caso particular, de la propuesta del proyecto de trabajo terminal.

COMENTARIO 2: La redacción del documento debería mejorar considerablemente para lograr un texto entendible, claro y, en el mejor de los casos, ameno. Como ya lo mencioné anteriormente la forma de estructurar las ideas no ayuda al entendimiento.

Comparto otros casos para ejemplificar:

1. En el segundo enunciado del primer párrafo de Introducción mencionan *"El problema del intercambio seguro de información es que nadie pueda entenderla excepto por el transmisor y el receptor"*. Esta redacción expresa que el hecho de que "nadie pueda entenderla" es un problema, cuando en realidad no lo es. De hecho, el problema del intercambio es que este se consume bajo algunos criterios de seguridad —que no se especifican, pero deben existir—, porque ocurre que o bien no se consume el intercambio *per se* o que se realice sin cumplir esos criterios de seguridad entonces el intercambio se podría calificar como no exitoso.
2. En el tercer enunciado de este mismo párrafo mencionan "El protocolo… es implementado sobre una curva elíptica…". Me deja la impresión de que "sobre" es una traducción literal de *"over"* donde el texto fuente podría ser algo como *"Diffie-Hellman protocol is implemented over elliptic curve…"*, sin embargo, en el español esta construcción no es la más apropiada para expresar que el protocolo se implemento "basado en" o "con base en" una cierta curva. Continuando el enunciado, se mención *"ofreciendo una gran seguridad"* con lo que se expresa que la acción mencionada en el enunciado, es decir, la implementación del protocolo en la curva elíptica tiene como consecuencia una mayor seguridad. Hasta este punto sigue sin entenderse con precisión lo que se debe entender por "seguridad" o que algo "sea seguro"; mientras este concepto sea ambiguo, el enunciado no aporta información.
3. En el cuarto enunciado de este mismo párrafo se menciona *"Esta técnica"* sin haber referido explícitamente a una técnica. En el siguiente enunciado se menciona *"Esto permite"* y en este punto de la lectura se ha utilizado excesivamente al sujeto tácito sin precisión de lo que se refiere.
4. El único enunciado del tercer párrafo inserta una coma entre el sujeto del enunciado y el predicado, partiéndolo sin una justificación evidente.
5. El tercer párrafo de la "Introducción" menciona *"Un estudio referente al presente, es el reforzamiento de autenticaciones en nubes públicas utilizando criptosistemas híbridos."*. De este texto interpreto, que existe un estudio que refiere al "presente", es decir, a este trabajo. Luego que ese estudio es "el reforzamiento de autenticaciones…". Como se puede ver la redacción no tiene un sentido claro. A lo largo del documento se hace referencia al "presente". No me quedó claro a que se refieren con este concepto. Acaso a la propuesta, al documento, al proyecto o ninguna de estas. Sugiero aclarar lo que se debe entender por el "presente".
6. En el segundo enunciado del primer párrafo de la sección *"Criptografía de curva elíptica…"*, la palabra *"numeros"* es esdrújula y, por lo tanto, debe estar acentuada. Aquí mismo se repite el texto "y puede ser", como un error menor. El siguiente 'enunciado' es *"Relativo a los esquemas de comunicación segura."* no expresa alguna idea.
7. En el según párrafo de la página 2, menciona *"Para cumplir con esta condición"* sin haber descrito la condición de la que habla.

COMENTARIO 3: Sugiero estudiar las nociones básicas de los temas involucrados, como requisito indispensable para la redacción de este documento. Algunas declaraciones realizadas en este documento, sugieren que no hay un entendimiento adecuado y, por lo tanto, se expresan algunos absurdos.

He aquí algunos ejemplos:

1. Ya mencionado anteriormente, el propósito de protocolo Diffie-Hellman no es distribuir llaves.
2. En el primer párrafo de la sección *"Criptografía de curva elíptica…"* menciona *"para nuestro propósito la curva elíptica es implementada sobre el conjunto de números discretos"*. Luego, en le punto 2 se hace referencia a la Figura 1 en donde se muestra gráficamente una curva elíptica que remite, al menos, a una idea donde la curva está definida en un espacio continuo, como $\mathbb{R}^2$, y no a uno discreto.

COMENTARIO 4: Las referencias actualmente expresadas tienen pocos datos para dar seguimiento. Sugiero tomar como referencia la documentación del paquete biblatex [1], particularmente la sección 2.1 y 2.2, en donde se pueden tener nociones más claras de la información que debe ser incluida dentro de las referencias y de acuerdo con el recurso que se esté refiriendo.

COMENTARIO 5: Sugiero volver a plantear los proyectos similares a que se esta proponiendo. En la sección titulada *"Sistemas similares que se han desarrollado son:"*, se presentan cuatro proyectos que se presumen similares al presentado sin dar datelles que sustenten porque se proponen como simlares o como referencias de este proyecto. No es posible saber en cuáles caracteristicas son similares o diferentes, qué pretende este proyecto mejorar respecto esos proyectos.

COMENTARIO 6: Considerando la redacción de este documento, he supuesto que este documento no fue revisado por los directores. Si este es el caso, entonces sugiero al estudiante apoyarse de sus directores, solicitándole revisiones periódicas de este documento y su trabajo en general, para poder obtener la retroalimentación adecuada que le permite realizar una redacción clara, concisa y correcta. Si bien la expresión escrita de los estudiantes pueden tener algunas deficiencias, la atención oportuna de los directores puede subsanar esas deficiencias y mejorar las habilidades escritas del estudiante.

[1]: http://mirrors.ctan.org/macros/latex/contrib/biblatex/doc/biblatex.pdf

=====

NOMBRE Y FIRMA DEL SINODAL:	Israel Buitrón Dámaso
ACADEMIA:	Ciencias Básicas
DEPARTAMENTO:	Formación Básica
CONTACTO:	ibuitron@ipn.mx www.comunidad.escom.ipn.mx/ibuitron/contacto.html