

General Introduction	01
1. Introduction.....	03
2. Web applications.....	03
2.1. 3-tier Architecture of web application.....	03
2.2. Web application security.....	04
2.2.1. SQL Injection.....	04
2.2.2. Cross Site Scripting (XSS).....	04
2.2.3. Broken Authentication and Session Management.....	04
2.2.4. Insecure Direct Object References.....	04
2.2.5. Cross Site Request Forgery (CSRF).....	05
2.2.6. Security Misconfiguration.....	05
2.2.7. Failure to Restrict URL Access.....	05
2.2.8. Invalidated Redirects and Forwards.....	05
2.2.9. Insecure Cryptographic Storage.....	05
2.2.10. Insufficient Transport Layer Protection.....	05
3. SQL injection.....	06
3.1. SQL injection Definition.....	06
3.2. Consequence of SQL injection.....	06
4. The SQL injection mechanisms.....	07
4.1. Parameter tampering.....	07
4.2. URL tampering.....	07
4.3. Cookie poisoning.....	08
4.4. Hidden field manipulation.....	08
4.5. HTTP header manipulation.....	09
5. SQL injection attack types.....	10
5.1. Tautologies.....	10
5.2. Logically incorrect queries.....	10
5.3. Union Query.....	10
5.4. Blind injection.....	11
5.5. piggy-backed queries.....	12
5.6. Stored procedure.....	12

5.7. Timing attacks.....	13
6. SQL injection prevention mechanism.....	13
6.1. Defensive coding practices.....	13
6.1.1.Input type checking.....	13
6.1.2.Encoding of inputs.....	13
6.1.3.Positive pattern matching.....	14
6.1.4.Identification of all input points.....	14
6.2. Black box testing.....	14
6.3. White box testing.....	14
6.4. Run time monitoring (control)	14
7. Existing solutions.....	14
7.1. Proxy filtering.....	14
7.2. AMNESIA.....	15
7.3. Client side validation.....	16
8. Conclusion.....	16
1. Introduction.....	17
2.Definition.....	17
3. basic Terminology.....	18
4. Functionality of work cryptography.....	18
5. Encryption and decryption.....	18
6. Common goals of cryptography.....	19
6.1. Message confidentiality.....	19
6.2.Message integrity.....	19
6.3.Authentication.....	19
6.4.Non-repudiation.....	19
7. Keys.....	19
8. Hash functions.....	20
8.1. Defintion.....	20
8.2.The hash function properties.....	21
8.3.1. Password Hashing.....	21
9. Digital signatuers.....	22
10. symmetric cryptography.....	23

10.1. Key Management.....	24
10.1.1. Static (or long-term) Keys.....	25
10.1.2. Ephemeral, or Session (or short-term) Keys.....	25
11.Public key cryptography.....	25
11.1. The RSA cryptosystem.....	25
11.1.1. The RSA encryption.....	26
11.1.2.The RSA decryption.....	26
11.1.3. The RSA signature.....	26
11.1.4. The RSA signature verifying.....	26
11.2. ECC cryptosystem.....	27
11.2.1. ECC encryptions/ decryption.....	28
11.2.2. Signature generation.....	28
11.2.3. Signature verification	28
11.3. The Elgamal cryptosystem.....	29
11.3.1.DL - discrete logarithm problem.....	29
11.3.2. Elgamel encryption.....	29
11.3.3.Elgamel decryption.....	30
11.3.4.Elgamel signature.....	30
11.3.5.Elgamal signature verification.....	30
Conclusion.....	30
1. Introduction.....	31
2. Existing solutions to preventing SQL injection use cryptography system.....	31
2.1. Mixture Secure Hashing technique and Advanced Encryption Standard (AES)....	31
2.1.1. Login phase.....	31
2.2. Preventing SQL injection attacks using Blowfish and RSA.....	32
2.2.1. Access Request Process.....	32
2.2.1.1. Registration.....	32
2.2.1.2. Login.....	33
2.2.2. Access grant process.....	34
2.3. Preventing SQL injection attacks using Multi-hashing.....	35
2.3.1. definition	35
2.3.2. Registration phase.....	35

2.3.2.1.First hash code.....	35
2.3.2.2.Second hash code.....	35
2.3.3. login phase.....	36
2.3.4. validation phase.....	36
2.4. Random algorithm.....	37
Conclusion.....	38
1. Introduction.....	39
2. Description of our proposed technique.....	39
2.1. Key generation.....	40
2.2. Registration phase.....	41
2.3. Login phase.....	42
3. Implementation.....	43
3.1. The developpement environnement.....	43
3.1.1. NetBeans IDE.....	43
3.1.2. Servlet.....	43
3.1.3. JSP definition.....	43
3.1.4. PHPmyadmin.....	44
3.2. The cryptographic library in JAVA.....	44
3.2.1. FlexiProvider.....	44
3.2.1.1. CoreProvider.....	44
3.2.1.2. ECProvider.....	45
3.2.2. mysql-connector-java-5.1.37-bin.....	45
3.2.3.Bouncycastle provider.....	45
3.3. Experimental results.....	45
4. Performance Evaluation.....	46
4.1. Digital signature time.....	46
4.2. Digital signature verification time.....	47
4.4. Memory usage.....	48
5. Results discussion.....	48
6.Conclusion.....	49
General Conclusion.....	50