# Content

1. Introduction
   1. Aims
   2. Motivation
2. Background
   1. PAKE
      1. Need for PAKE
      2. What is PAKE
   2. EKE
      1. What is EKE
      2. EKE protocol design
3. Design
   1. Diffie-Hellman key exchange
      1. DH parameters
      2. How it works
      3. Parameter selection
      4. Need for encryption - EKE
   2. Parameter selection
4. Implementation
   1. Challenges
      1. Large number operations
         1. Miller rabin test
         2. Modular Exponentiation
      2. Primitive root for large numbers – done in 3a
         1. Math behind it
      3. KDF scrypt
5. Evaluation
6. Conclusion

# 2

## (a)PAKE

### 2.a (i) Need for PAKE

The most common method employed for ensuring secure communications over the Internet is TLS (Transport Layer Security).

The TLS connection commences with a TLS handshake wherein the parties agree on the encryption algorithm and cryptographic parameters, generate the shared secret key, and authenticate each other. In simpler terms, an agreement is reached on the communication method, and mutual authentication is performed. Messages can then be encrypted and transmitted through a confidential TLS channel. The server can decrypt a message sent by the client and also verify its integrity. Subsequent to decryption, the server gains access to the original plaintext message.

When this mechanism is utilized for password authentication, the password is sent by the client to the server using the confidential TLS channel. The server decrypts the password and verifies it against a one-way hash image of the password (since the hash of the password and the salt to calculate the hash are stored in the database). This way, if access to the database is gained by an attacker, they only obtain the hash value. Consequently, they will need to execute an exhaustive offline dictionary attack to deduce the password.

However, this method possesses an Achilles' heel - the user transmits their cleartext password to the server as it is required for the server to conduct the check. If the TLS connection is established with a compromised server, an attacker might discover the user's password that appears in clear text.

PAKE provides a solution where the password does not have to be sent to the server in cleartext.

### 2.a(ii) What is PAKE

PAKE, an acronym for Password Authenticated Key Exchange, represents a protocol facilitating the establishment of a shared secret key between two parties for the purpose of secure communication. The key is formed over an untrusted network, with each party authenticating each other through a password, ensuring that the password is not transmitted in cleartext to the server. The key exchange is secure even when the messages exchanged are fully observable by a potential attacker.

In the context of PAKE, the authentication password is short and easily memorizable. The protocol's structure is designed in a manner that eliminates the necessity for the password to be uniformly distributed over a large space to ensure security. This property makes it more convenient than alternative authenticated key exchange protocols.

Nevertheless, numerous PAKE protocols remain susceptible to dictionary attacks, wherein an attacker tries all possible passwords to compromise security (brute-force method). Consequently, these protocols should account for the fact that the passwords used have low entropy.

## (b) EKE

### What is EKE

The encrypted key exchange (EKE) protocol of Bellovin and Merritt was the first successful PAKE protocol.

It is a combination of asymmetric (public key) and symmetric cryptography (private key). Two parties can use a shared secret (password) to exchange secret information like the session key. The password is protected from offline dictionary attacks. The protocol is also secure against active attacks.

### EKE protocol design

We assume that parties A and B, with public keys E\textsubscript{A} and E\textsubscript{B}, share the password P. \\

A then sends encryption of E\textsubscript{A} using P\\

i.e., \hspace{1in} P(E\textsubscript{A})\\

B decrypts it and generates a random secret key R. Subsequently, B sends the encryption of R using E\textsubscript{A} and P \\

i.e., \hspace{1in} P(E\textsubscript{A}(R)) \\

A decrypts this message to obtain the common secret key R.\\

A and B proceed to send each other challenges encrypted using R to validate R (check that they have arrived at the same secret key). Hence, A sends an encrypted challenge\textsubscript{A} \\

i.e., \hspace{1in} R(challenge\textsubscript{A}) \\

B decrypts this and reciprocates by sending its own challenge to A along with the decrypted challenge.\\

i.e., \hspace{1in} R(challenge\textsubscript{A}, challenge\textsubscript{B}) \\.

A then decrypts this. If the decrypted challenge\textsubscript{A} matches the original one, everything is okay. Then A sends back challenge\textsubscript{B} \\

i.e., \hspace{1in} R(challenge\textsubscript{B}) \\

B then decrypts it. If it matches the original challenge sent, both parties are confident that they have arrived at the same secret key, which they can now use for communication.

### EKE implementations

EKE can be implemented using RSA or using El Gamal encryption, which is an encrypted version of Diffie-Hellman key exchange.\\

I chose to implement EKE based on Diffie-Hellman.

# 3

## DH Key exchange

The EKE protocol represents an encrypted version of the Diffie-Hellman key exchange. Therefore, to comprehend the design of EKE, it is first necessary to grasp how the Diffie-Hellman key exchange works.

\\

The Diffie-Hellman key exchange facilitates the derivation of a shared key by two parties through the exchange of messages, without the need to transmit the private key within the message.

### DH parameters

Two parties, A and B, generate random numbers denoted as R\textsubscript{A} and R\textsubscript{B}, respectively. These random values are kept confidential and are not disclosed to the other party.\\

Additionally, an agreement is reached on a modulus, p, and a generator, g.\\

p is a safe prime and g is its primitive root. These parameters are shared publicly. Consequently, A and B have the same values of p and g, which are publicly known.

### How it works

The steps in the key exchange process are described below.

\begin{enumerate}

\item A sends its public key to B. The public key is calculated by raising the generator to the private random number R\textsubscript{A} and the calculating its modulus with p.\\

A sends \hspace{1in} E\textsubscript{A} = g\textsuperscript{R\textsubscript{A}} mod p \hspace{1in} (public key of A)

\item B receives A's public key and uses it to calculate the shared secret key R. It does this by raising A's public key to the secret number R\textsubscript{B} known only to B.

\begin{displaymath}

R = E\_A^{R\_B} (mod p)

= (g^{R\_A} (mod p))^{R\_B} (mod p)

= (g^{R\_A})^{R\_B} (mod p)

= g^{R\_A R\_B} (mod p)

\end{displaymath}

\item B sends its public key to A.\\

B sends \hspace{1in} E\textsubscript{B} = g\textsuperscript{R\textsubscript{B}} mod p \hspace{1in} (public key of B)

\item A receives B's public key and uses it to calculate the shared secret key R in the same way as B.

\begin{displaymath}

R = E\_B^{R\_A} (mod p)

= (g^{R\_B} (mod p))^{R\_A} (mod p)

= (g^{R\_B})^{R\_A} (mod p)

= g^{R\_A R\_B} (mod p)

\end{displaymath}

\item As we can see, both A and B have calculated the same value for R. Hence, they have calculated the same secret key which they can now use to exchange information securely.

\end{enumerate}

### Parameter Selection

The parameters are modulus p and generator g.\\

p needs to be a safe prime. A safe prime is defined as follows.

Let's say q is a prime number. If \begin{math} p = 2q + 1\end{math} is also prime, then we say that p is a safe prime. [2]

This property is required to ease the process of finding the primitive root. \\

\\

g is a primitive root of p.\\

Given a positive integer n, we say that $a \in Z$ with gcd(a,n) = 1 (i.e., a and n are co-prime integers), is a primitive root modulo n if the multiplicative order of a modulo n is equal to $\phi (n)$. [5]\\

$\phi (n)$ represents Euler's Totient function. Since p is prime, $$\phi (p) = p - 1$$

Multiplicative order of a modulo n is the smallest positive integer k such that $$ a^k \equiv 1 (mod n)$$ [5]

Hence, g will be a primitive root of p, if $$ k = p-1$$ where k is the multiplicative order of g.

\\

To actually find the generator g, we use the knowledge of quadratic residues. An integer q is called a quadratic residue modulo n if it is equivalent to a perfect square modulo n; i.e., if there exists an integer x such that $$ x^2 = q (mod n)$$

If a number is not a quadratic residue, it is called a quadratic non-residue.[4]\\

The generator g should be a quadratic non-residue modulo n. This can be checked using Legendre symbol.\\

Let n be an odd prime and a be an integer. Legendre symbol is a function defined as $$ (\frac{a}{n}) \equiv a^{\frac{n-1}{2}}\;(mod n) \;\; and \;\; (\frac{a}{n}) \in \{-1,0,1\}$$ [3]

The value of the Legendre symbol is \begin{itemize}

\item 0: If $a \equiv 0 \; (mod \; n)$

\item 1: If a is a quadratic residue modulo n and $a \neq 0 \; (mod \; n)$

\item -1: If a is a quadratic non-residue modulo n

\end{itemize}

Hence, generator g is a number with Legendre value -1 ,i.e., $$ (\frac{g}{p}) = -1$$

### Need for encryption – EKE

The Diffie-Hellman key exchange, while a powerful method for establishing shared secret keys, lacks a built-in mechanism for authentication, rendering it vulnerable to Man-in-the-Middle (MitM) attacks. In a MitM scenario, the adversary can intercept the communication between two parties, A and B, with the potential to eavesdrop on and alter the exchanged messages.

Upon A transmitting its public key to B, the attacker intercepts and dispatches its own public key to B. Similarly, when B forwards its public key to A, the same substitution is executed. Subsequently, A and B derive separate shared secret keys with the attacker under the false impression that it is derived between themselves (A and B). Having successfully established discrete connections with both A and B, the attacker makes them believe a mutual connection has been forged. Consequently, A and B mistakenly perceive themselves as engaged in direct communication with each other, when, in truth, the adversary manipulates and governs the discourse.

The EKE protocol serves as a preventive measure against such subversion by introducing authentication. It mandates that the two parties possess the same password as a prerequisite for establishing a shared secret key. Hence, the attacker, without knowledge of the password, cannot perform this attack.