TC
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

YMH459 YAZILIM MÜHENDİSLİĞİ GÜNCEL KONULAR DERSİ PROJESİ
MİMARİ DOKÜMAN

Proje Adı

CRYPIT(Fotoğraf Şifreleme için Mobil Uygulama)

Proje Logosu

Proje Ekip Lideri

SÜMEYYE GÜLNUR DADAK (16542503)

Proje Çalışma Grubu

ABDULKADİR DOĞANER (16541563)
ARZU KÜBRA YILAR (175541031)
BERNA UZUNOĞLU (16542513)
ENİS CAN YILMAZ (15541531)
HÜSEYİN BİTİKÇİ (16541509)
İHSAN CENKIZ (175541022)
İSMAİL ÇAĞAN (16541542)
KÜBRA ATICI (14545522)
MEHMET CAN AKKAŞ (14542518)
MEHMET FURKAN KEMALLI (185541087)
MERT BEKTAŞ (16541522)
MUSTAFA ENES ÖZÇELİK (175541068)
TUGAY AYAR (15542514)

Proje Yürütücüleri

Doç. Dr. Fatih ÖZKAYNAK

ELAZIĞ
2020-2021

İÇİNDEKİLER

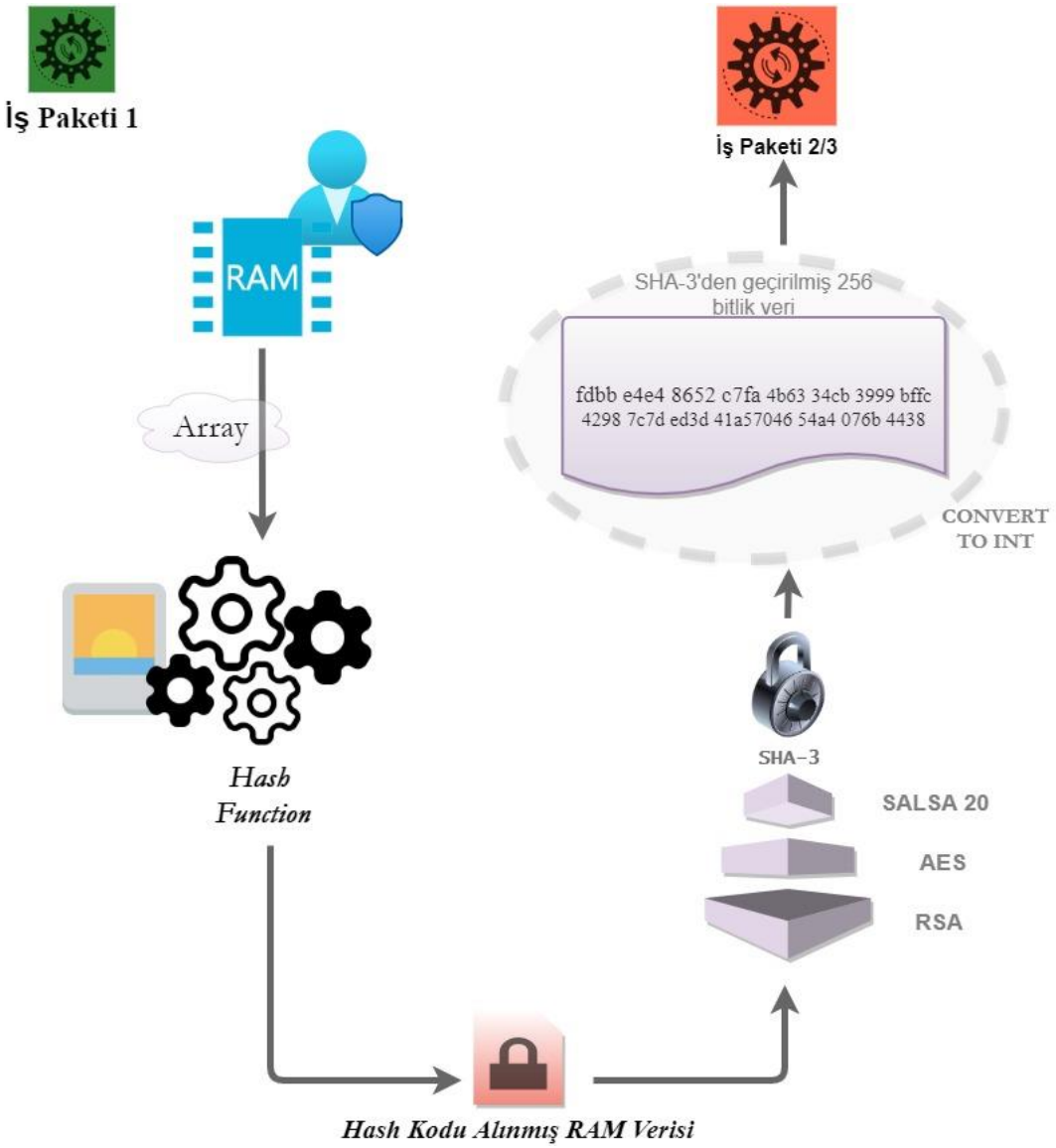
1 İŞ PAKETLERİ MİMARİ YAPISI 3
1.1 İş Paketi 1 Mimari Yapısı 3
1.1.1 İş Paketi 1 Akış Şeması 4
1.2 İş Paketi 3 Mimari Yapısı 5
1.2.1 İş Paketi 3 Akış Şemaları 6
1.3 İş Paketi 4 Mimari Yapısı 9
1.4 İş Paketi 5 Mimari Yapısı 10
1.4.1 İş Paketi 5 Akış Şemaları 11
2 GERÇEKLEŞTİRİLEN SİSTEMİN GENEL MİMARİSİ 19

ŞEKİLLER

Şekil 1- İş Paketi 1 Mimari Yapısı 3
Şekil 2- İş Paketi 1 Akış Şeması 4
Şekil 3- İş Paketi 3 Mimari Yapısı 5
Şekil 4- İş Paketi 3 randomBin() Akış Şeması 6
Şekil 5- İş Paketi 3 randArr() Akış Şeması 7
Şekil 6 - İş Paketi 3 createReceiverKey() Akış Şeması 8
Şekil 7- İş Paketi 4 Mimari Yapısı 9
Şekil 8- İş Paketi 5 zigzag1() Akış Şeması 11
Şekil 9- İş Paketi 5 decimaltoBinary() Akış Şeması 13
Şekil 10- İş Paketi 5 division() Akış Şeması 14
Şekil 11- İş Paketi 5 xor() Akış Şeması 15
Şekil 12- İş Paketi 5 byteConversion() Akış Şeması 16
Şekil 13- İş Paketi 5 zigzag() Akış Şeması 17
Şekil 14- İş Paketi 5 ters() Akış Şeması 18
Şekil 15- Gerçekleştirilen Sistemin Genel Mimarisi 19

1 İŞ PAKETLERİ MİMARİ YAPISI

1.1 İş Paketi 1 Mimari Yapısı



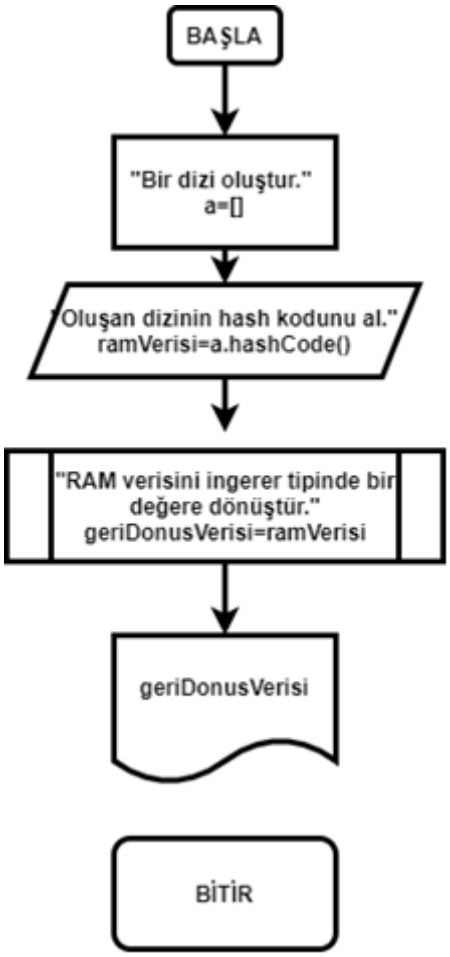
Şekil 1- İş Paketi 1 Mimari Yapısı

İş paketi 1 üzerinden RAM verisini ve kullanılmak istenen imgeyi okuyarak bir dizi içerisinde tutulduktan sonra Hash fonksiyonundan geçirilmektedir. Bu şekilde Hash kodu alınmış bir RAM verisi elde etmiş olunmaktadır. Daha sonra bu veri şifreleme algoritma standartlarından SHA-3, SALSA 20, AES, RSA fonksiyonlarından geçirilerek 256 Bit veri oluşturulmaktadır. Ve geri dönüş olarak bir int değer İş Paketi 2 -3 gönderecek şekilde bir çıktı değeri elde edilmektedir.

1.1.1 İş Paketi 1 Akış Şeması

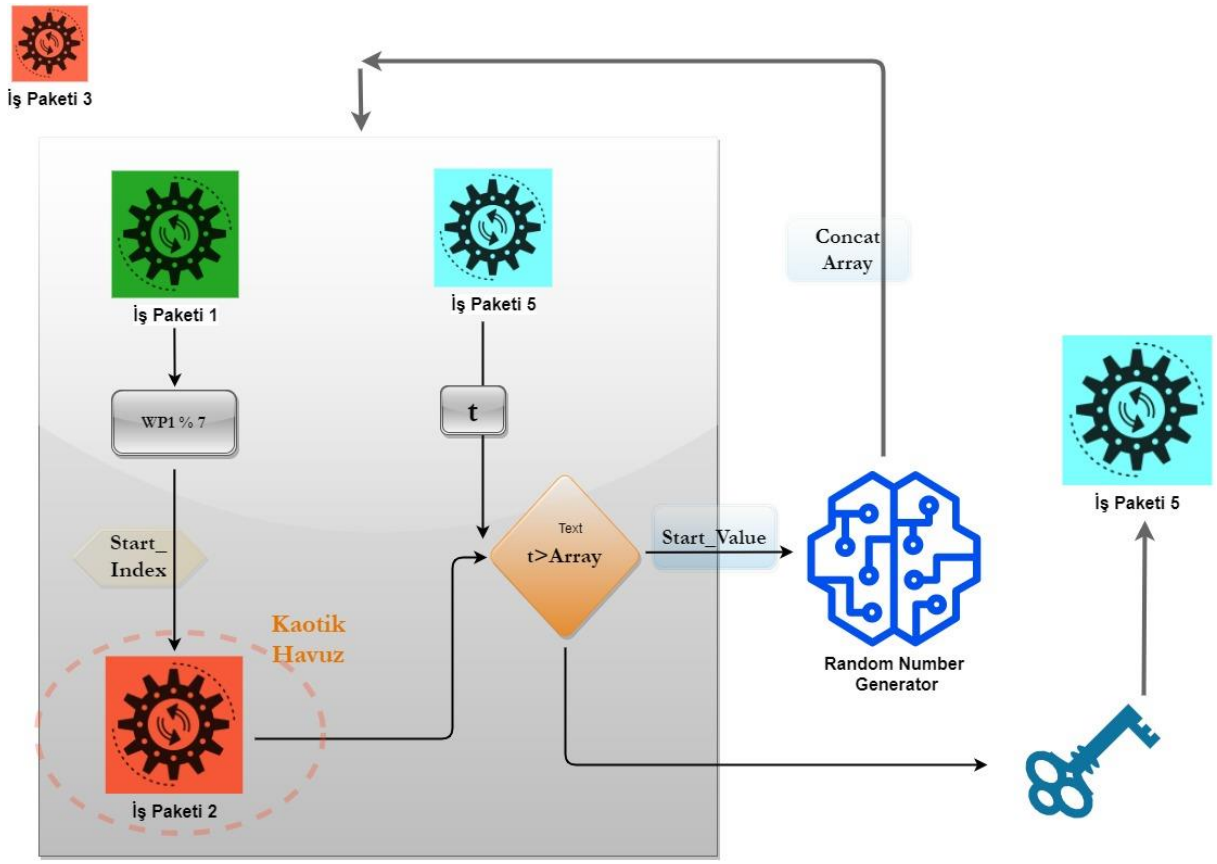
Paket Kapsamında Görev Alanlar:

- İSMAİL ÇAĞAN
- TUGAY AYAR
- ABDULKADİR DOĞANER
- MEHMET CAN AKKAŞ



Şekil 2- İş Paketi 1 Akış Şeması

1.2 İş Paketi 3 Mimari Yapısı



Şekil 3- İş Paketi 3 Mimari Yapısı

İş Paketi 3 ' de İş Paketi 1'den gelen değere Mod 7 (WP1%7) uygulanarak başlangıç indeksi oluşturulmaktadır. Daha sonra İş Paketi 2 içerisinde yer alan kaotik havuzda başlangıç indeksi kullanılarak anahtar üretimi için gereken başlangıç değeri elde edilmektedir. Anahtar uzunluğunu belirlemek için İş Paketi beşten imgenin boyutunu ifade eden t (3* height*witdth*8)değeri ile boyut kontrolü yapılmaktadır. Bu başlangıç değerleri ile Rundom Number Generator ile 1 milyon adet rasgele bit üretilmekte ve bu bit dizeleri birleştirilerek geri döndürülmektedir. İhtiyaç olan kadar bit ile anahtar üretilerek İş Paketi – 5 anahtar(key) iletilmektedir.

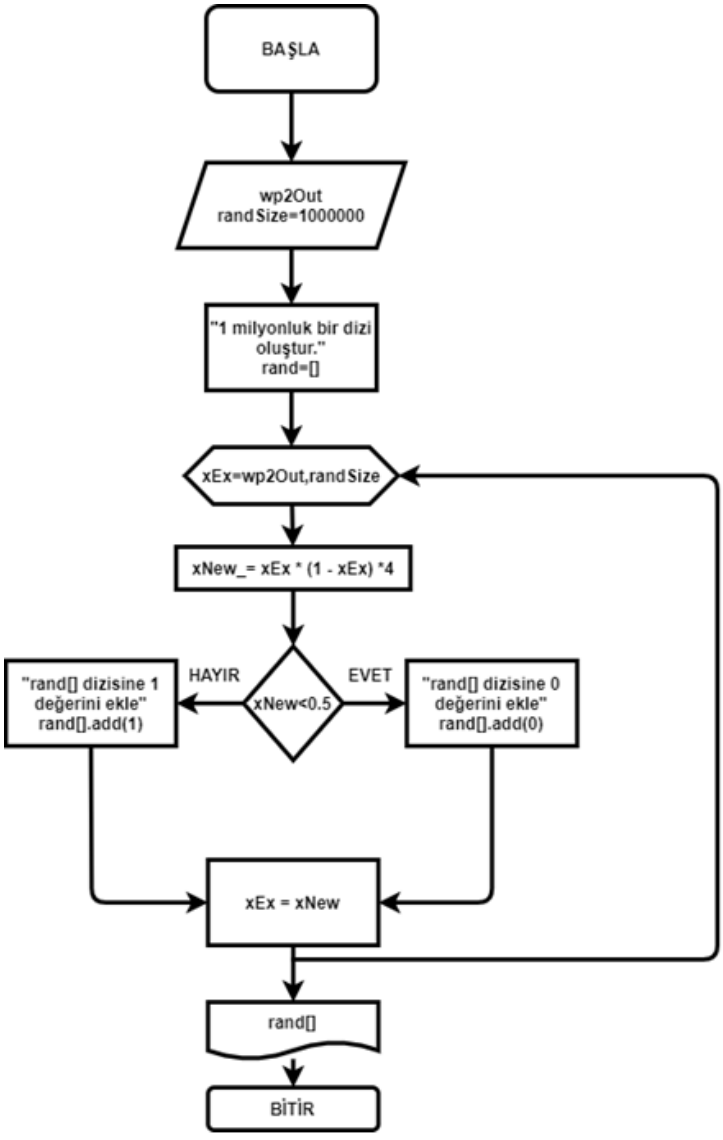
1.2.1 İş Paketi 3 Akış Şemaları

Paket Kapsamında Görev Alanlar:

- MUSTAFA ENES ÖZÇELİK
- BERNA UZUNOĞLU
- ARZU KÜBRA YILAR
- İHSAN CENKIZ

1.2.1.1 İş Paketi 3 randomBin(wp2Out) Akış Şeması

Bu fonksiyonda parametre olarak alınan başlangıç değeri ile 1 milyon adet rastgele bit üretilmekte ve bu bitler dizi ile geri döndürülmektedir.

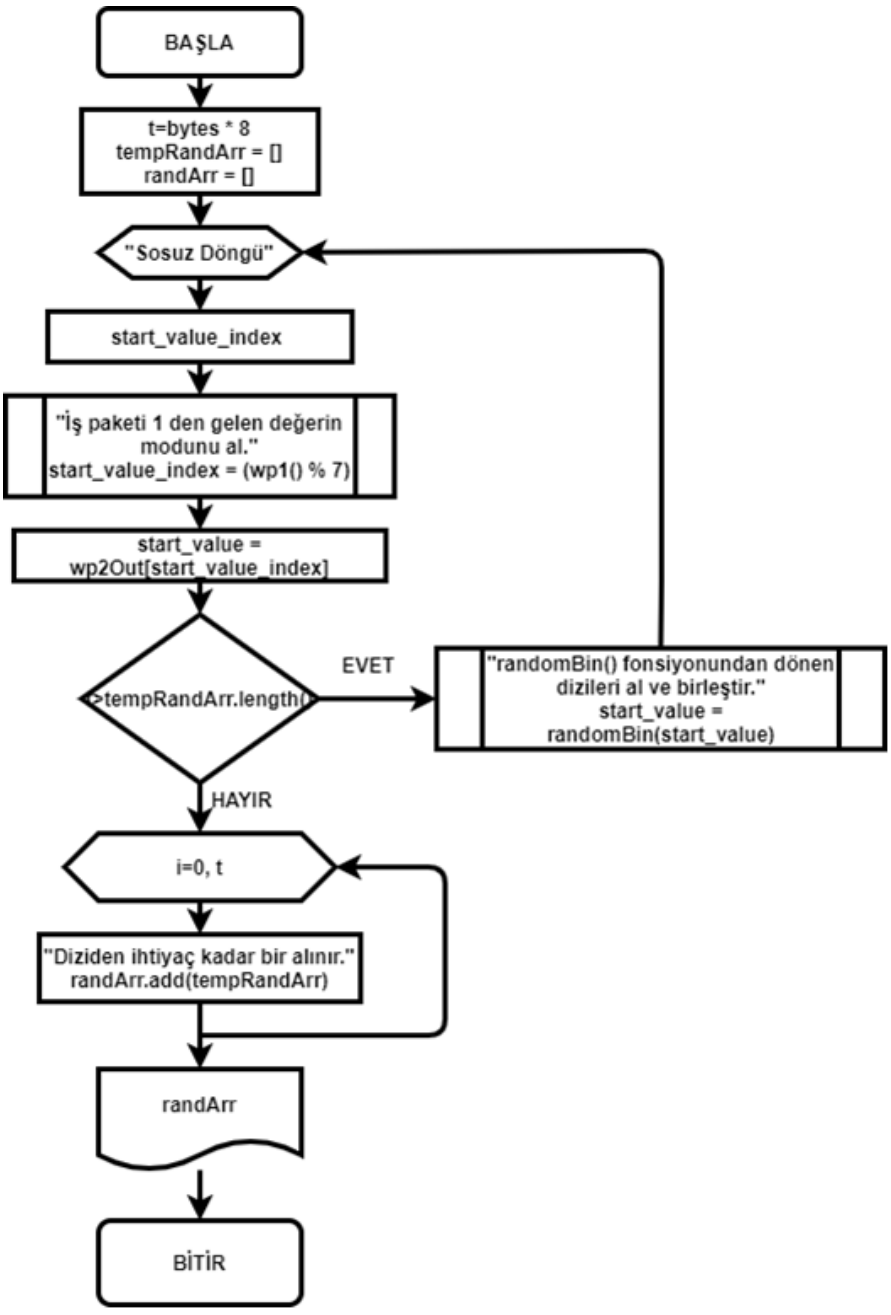


Şekil 4- İş Paketi 3 randomBin() Akış Şeması

1.2.1.2 İş Paketi 3 randArr(wp2Out, bytes)

Bu fonksiyonda genel anahtar oluşturmak için her 1 milyon bitte bir randomBin() fonksiyonu çağırılmıştır. Gelen bytes parametresine göre anahtar uzunluğunu belirleyerek oluşan bir milyon bitlik dizileri birleştirip içinden ihtiyaç olan kadar biti başka bir diziye aktararak geri döndürür.

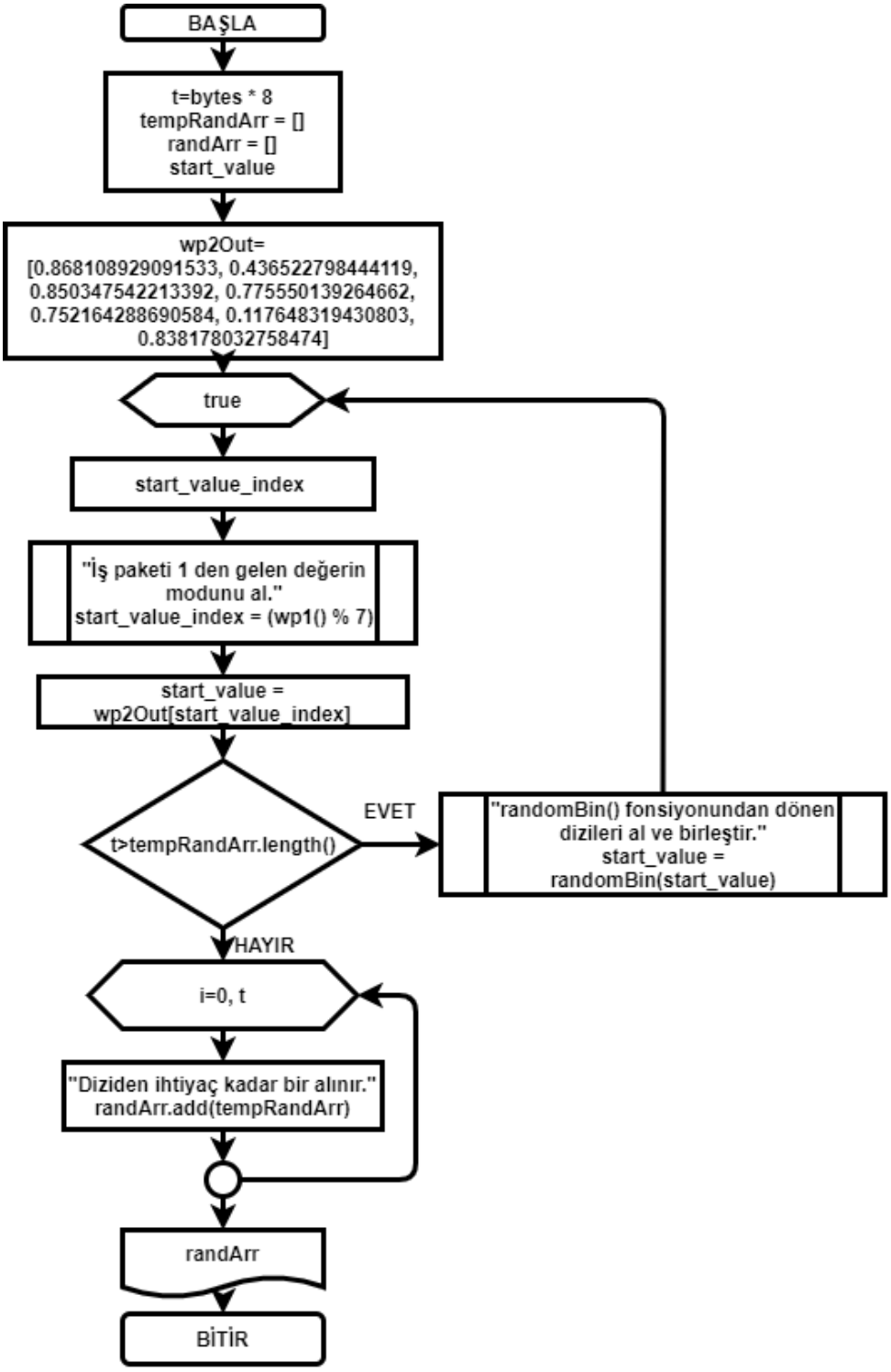
1.2.1.3 İş Paketi 3 randArr() Akış Şeması



Şekil 5- İş Paketi 3 randArr() Akış Şeması

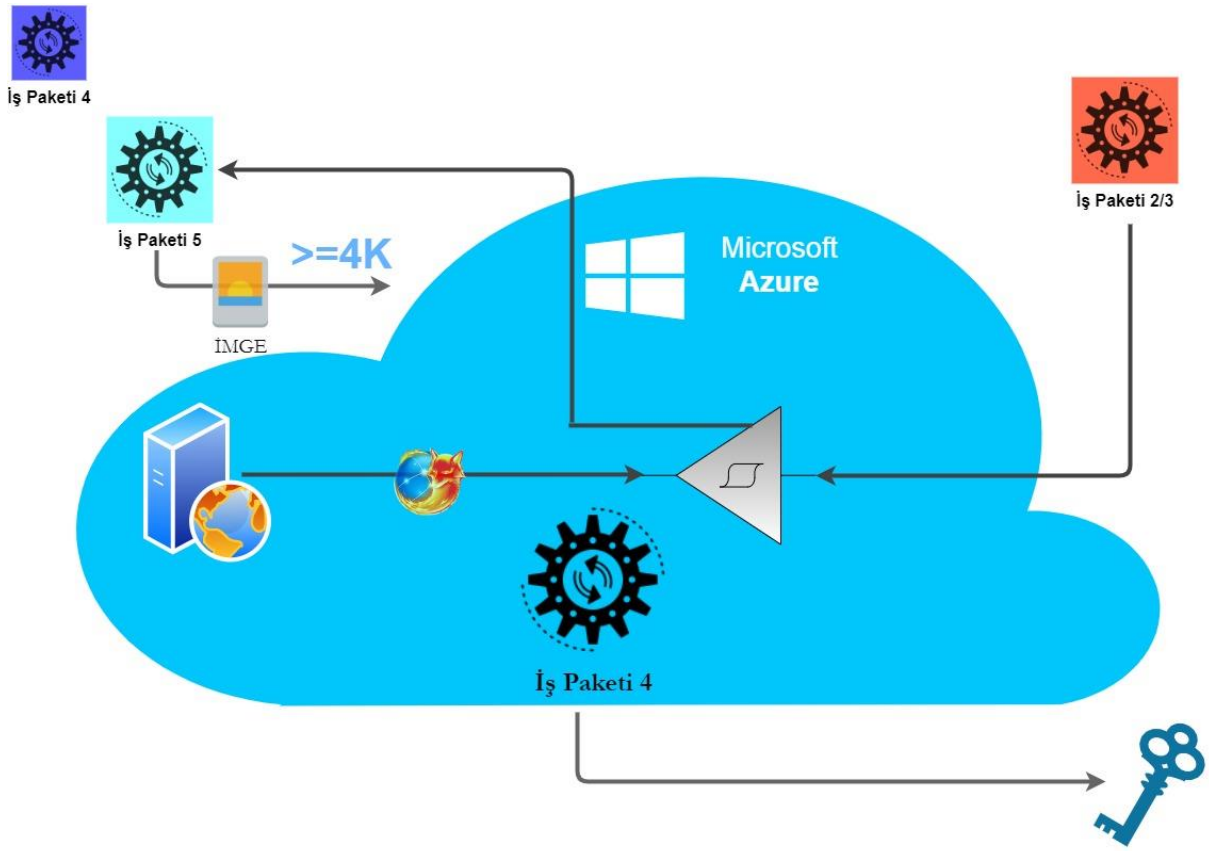
1.2.1.4 İş Paketi 3 createReceiverKey(start_values_indices, bytes)

Bu fonksiyon alıcı kullanıcının aldığı resmi yeniden deşifre edebilmek için üretilmesi gereken anahtarı üreten fonksiyondur. Parametre olarak başlangıç değerlerinin indis değerini ve byte değerini alır.



Şekil 6 - İş Paketi 3 createReceiverKey() Akış Şeması

1.3 İş Paketi 4 Mimari Yapısı



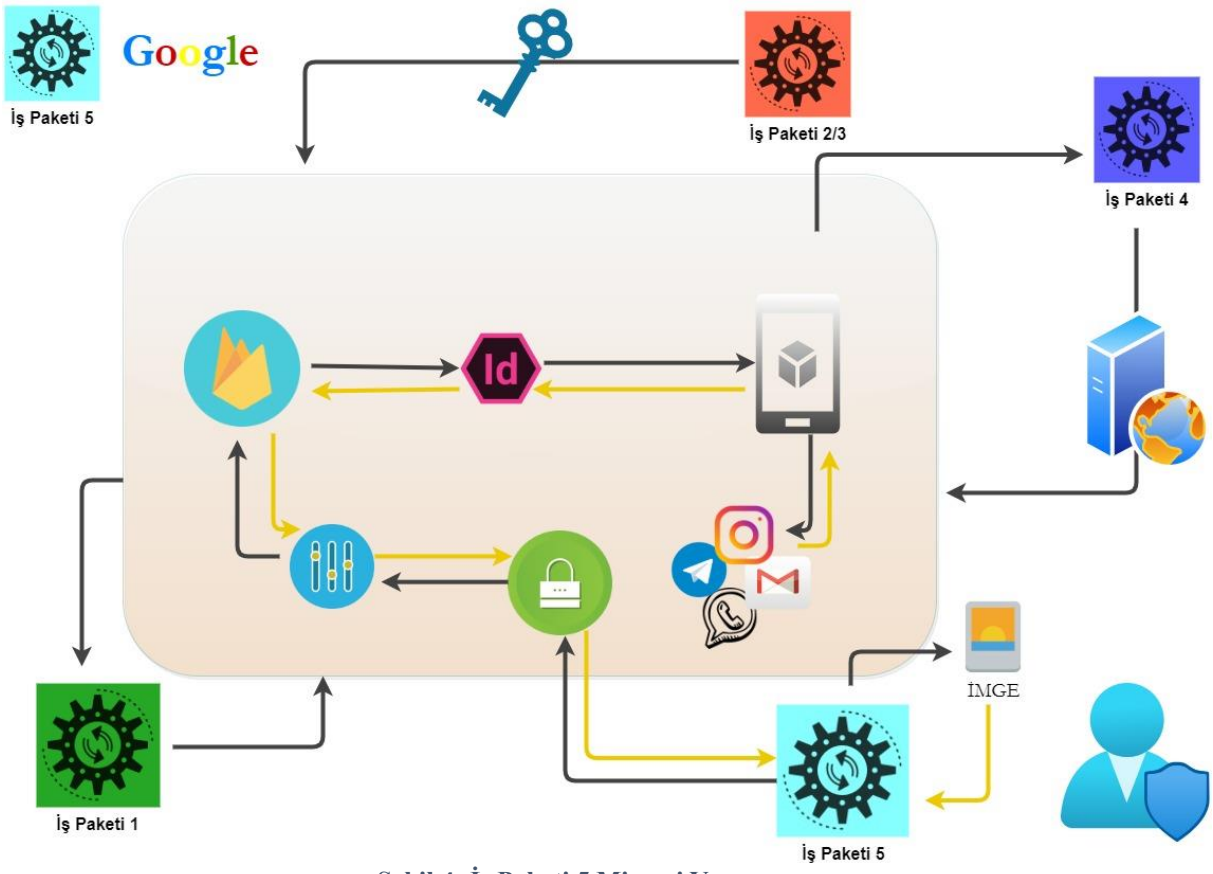
Şekil 7- İş Paketi 4 Mimari Yapısı

İmgenin boyut verisi 4K ve üzeriyse İş paketi 5 tarafından çalış komutu alan bu sistem, genel sistemin yorulmaması ve daha verimli çalışması için oluşturulmuştur.Boyut verisi 4k ve üzeriyse restfull API haberleşmesi üzerinden oluşturduğumuz server içerisindeki trigger tetiklenerek anahtar burada , algoritmasını iş paketi 3 ten aldığı fonksiyon ile üretilecektir ve anahtar iş paketi 5 e sunulacaktır.

Paket Kapsamında Görev Alanlar:

- MERT BEKTAŞ
- MEHMET FURKAN KEMALLI
- KÜBRA ATICI

1.4 İş Paketi 5 Mimari Yapısı



Şekil 4- İş Paketi 5 Mimari Yapısı

İş Paketi 5 tüm sistemin başlangıcı ve sonu olarak görev almaktadır. Tüm iş paketlerinin birleştirildiği ve veri alışverişinde bulunduğu bu iş paketi üzerinde asıl amaç ara yüz tasarımının yanı sıra performansı ve uygulamanın dışarıya açılan kapılarının güvenliğini sağlamaktır. Seçilen ya da çekilen imgenin datasına erişilir , erişilen bu data kendi dolaşma yöntemimiz olan bir zigzag fonksiyonuna tabi tutulur. Boyutu hesaplanıp iş paketi 3 e buna göre bir anahtar üretmesi söylenir. Erişilen ve karıştırılan bu baytlar önce bitlerine daha sonra anahtarla aynı boyutta olması için bir tamamlama fonksiyonuna dizi olarak verilir. Ardından iş paketi 3 ten gelen anahtar ile birlikte bu tamamlanan dizimiz xor fonksiyonuna tabi tutulur. Buradan çıkan dizi başlangıç koşulları ile birlikte googleFirebase de oluşturduğumuz veri tabanına gönderilir. Gönderilen bu veriler bir dokümana kaydedilir. Kaydedilen dökümanın ID si kullanıcıya sunulur. Kullanıcı dilediği platformdan bu ID yi paylaşabilir. Karşı tarafta ulaşan ID ile görüntüyü elde etmek için textfield dan aldığımız veri aynıdır. ID firebase e yollanır. Orada ki dökümanın içindeki başlangıç koşullarımız iş paketi 3 e , xorlu dizi iş paketi 5 e ulaştırılacak şekilde yol haritası çizilir. İş paketi 5 e gelen xorlu dizi tersine fonksiyonlarından geçerek , xor fonksiyonundan önceki halini alır. Gelen anahtarla tekrar xor işlemine tabi tutulduğunda bize imgenin datasını verir. Data , gerekli okutma fonksiyonuna verilerek imge yeniden oluşturulur ve ekrana bastırılır. Eğer ki boyutumuz 4K dan büyükse azure platformunda oluşturduğumuz server içerisindeki trigger devreye girer ve anahtarımız sistemi yavaşlatmamak için orada üretilir.

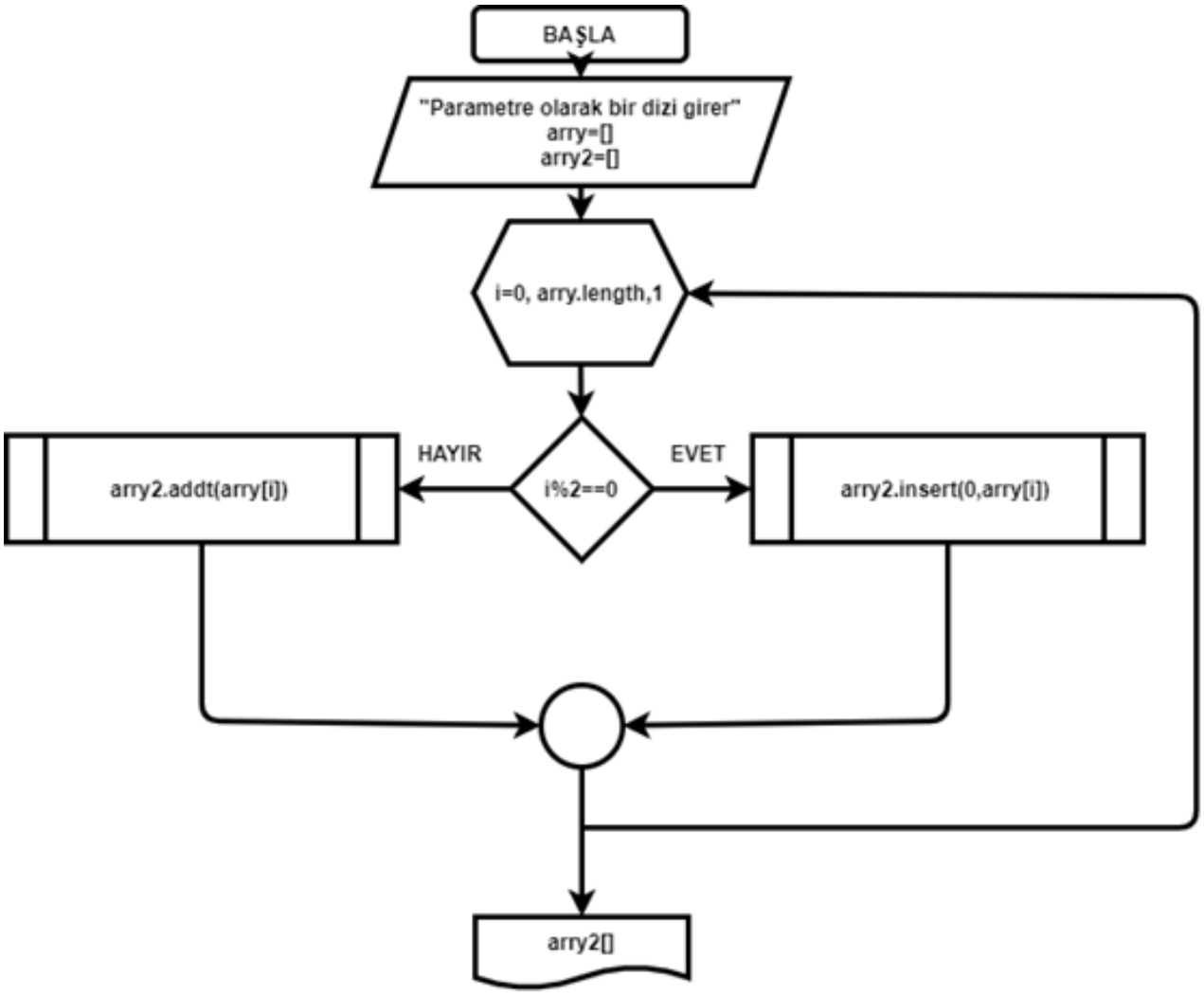
1.4.1 İş Paketi 5 Akış Şemaları

Paket Kapsamında Görev Alanlar:

- SÜMEYYE GÜLNUR DADAK
- HÜSEYİN BİTİKÇİ
- ENİS CAN YILMAZ

1.4.1.1 İş Paketi 5 zigzag1(arry) Akış Şemaları

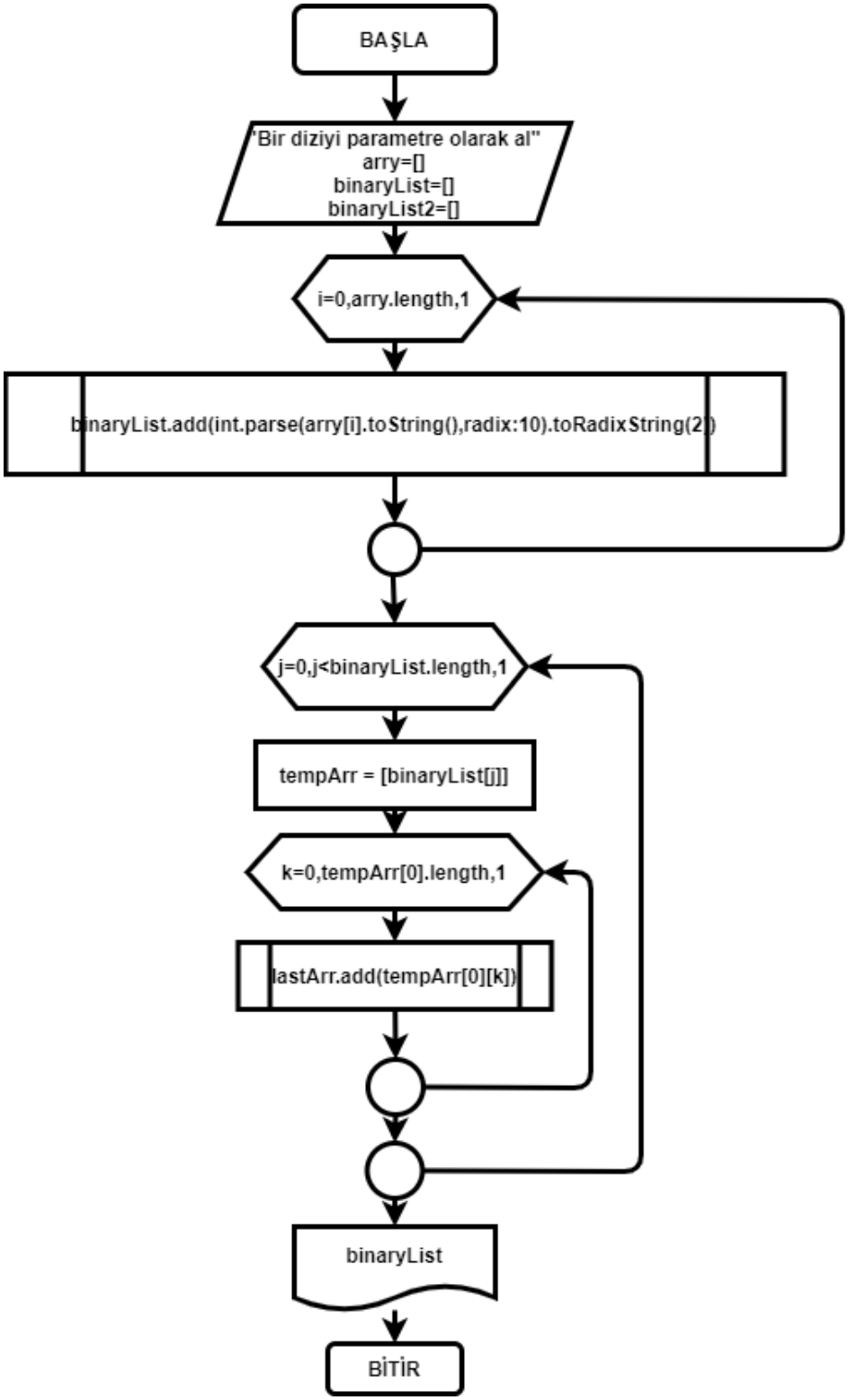
Bu fonksiyon bayt verilerine ayrılmış dizinin zig-zag şeklinde gezilerek tek boyuta indirgenmiş, yani karıştırılmış diziyi elde etmek için yazılmıştır.



Şekil 8- İş Paketi 5 zigzag1() Akış Şeması

1.4.1.2 decimaltoBinary(arry) Akış Şeması

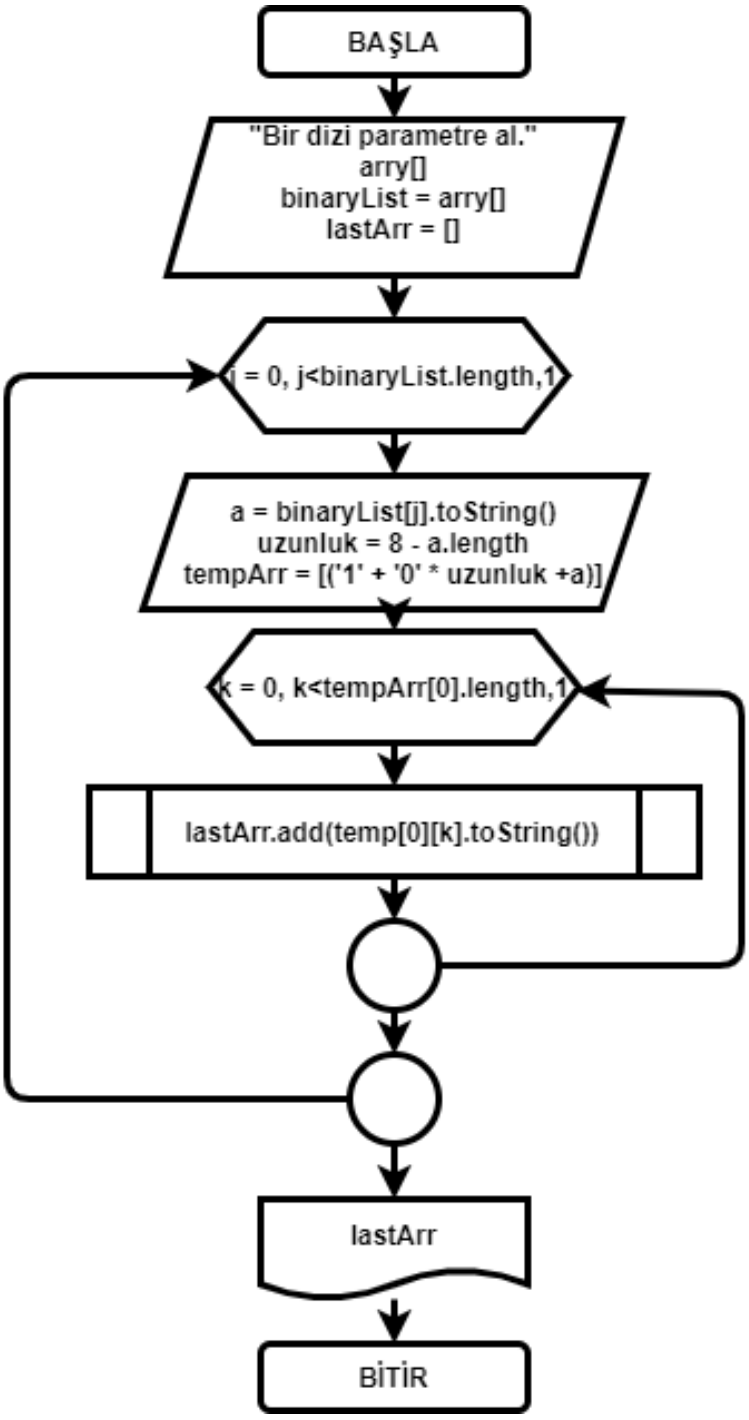
Bu fonksiyon zigzag fonksiyonundan çıkan tek boyutlu karıştırılmış byte dizisindeki byte değerlerini binary ye çevirme işlemi için yazılmıştır.



Şekil 9- İş Paketi 5 decimaltoBinary() Akış Şeması

1.4.1.3 division(arry) Akış Şeması

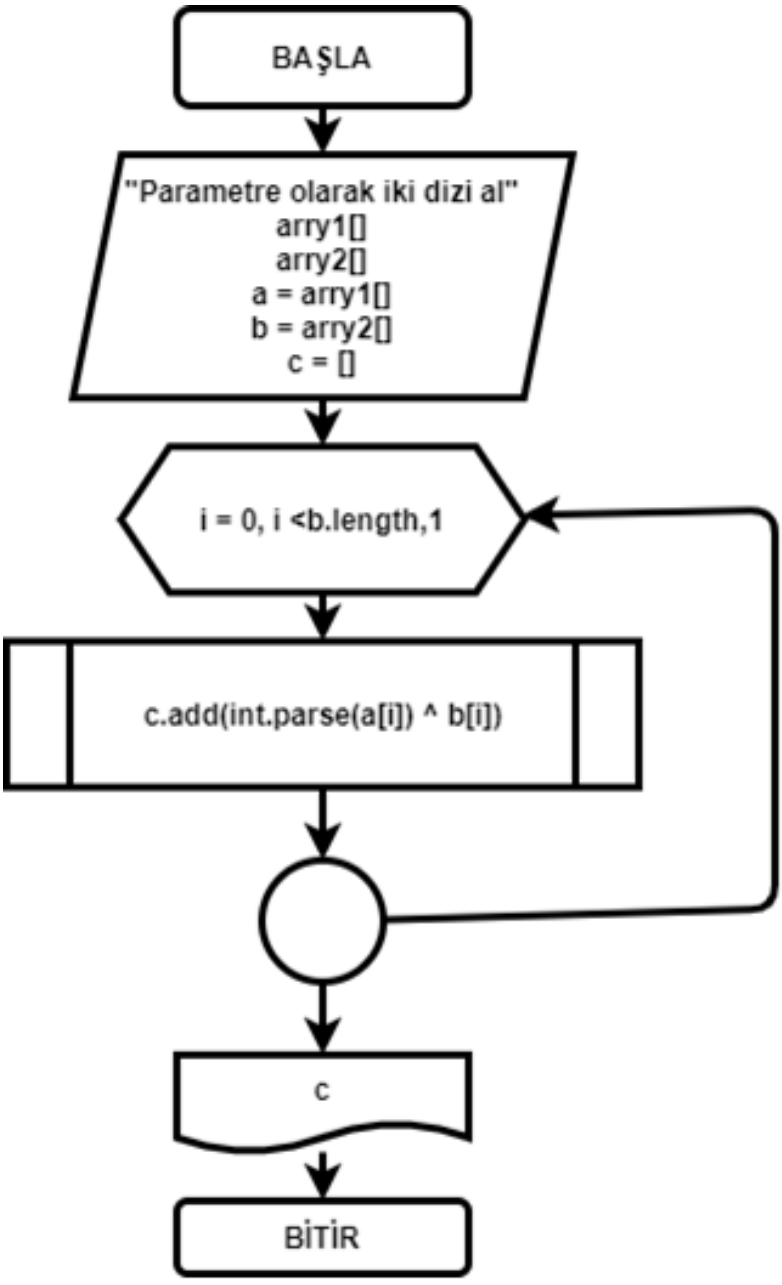
Bu fonksiyonda decimaltoBİnary() fonksiyonundan çıkan binary değerleri XOR işlemine hazırlamak için 8 karaktere tamamlamak, yani tüm sekizli olması gereken ancak olmayan dizi elemanlarının başına "0" değişkeni ekleyerek işleme hazır hale getirilmesi için yazılmıştır.



Şekil 10- İş Paketi 5 division() Akış Şeması

1.4.1.4 xor(arry1, arry2) Akış Şeması

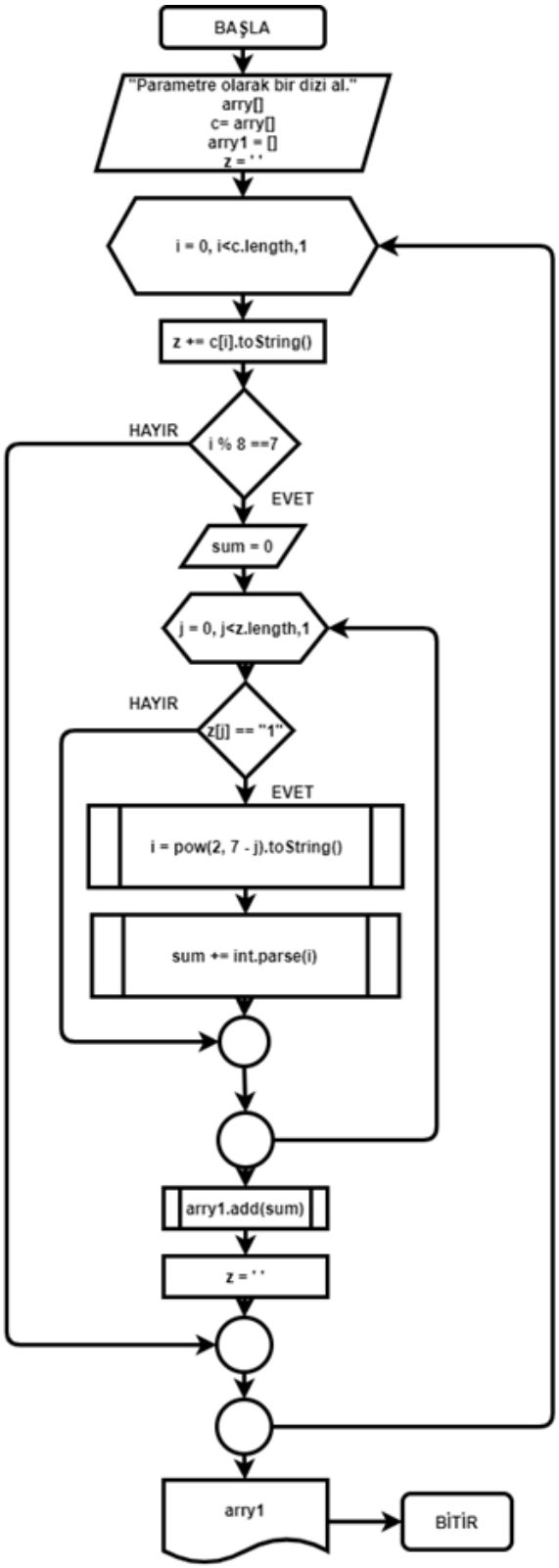
Bu fonksiyon anahtar ve resimden elde edilen binary dizileri parametre olarak alıp kriptolojide önemli bir yeri olan XOR işlemine tabi tutarak yeni bir dizi oluşturmak için yazılmıştır.



Şekil 11- İş Paketi 5 xor() Akış Şeması

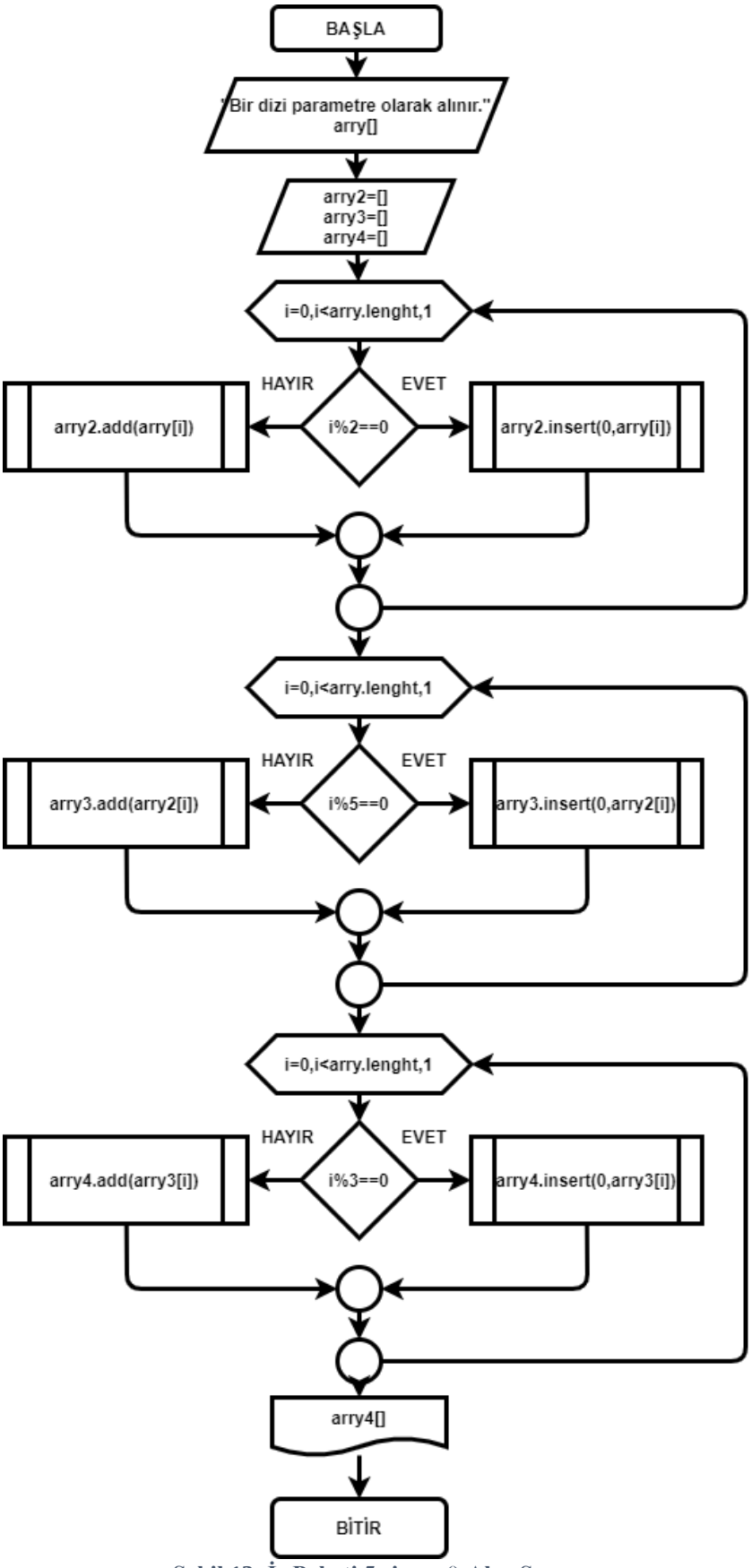
1.4.1.5 byteConversion(arry) Akış Şeması

Bu fonksiyon üretilen şifrelenmiş veriden oluşan binary dizisini sekizli gruplar halinde alarak birleştirip byte dizisi oluşturmak için yazılmıştır.



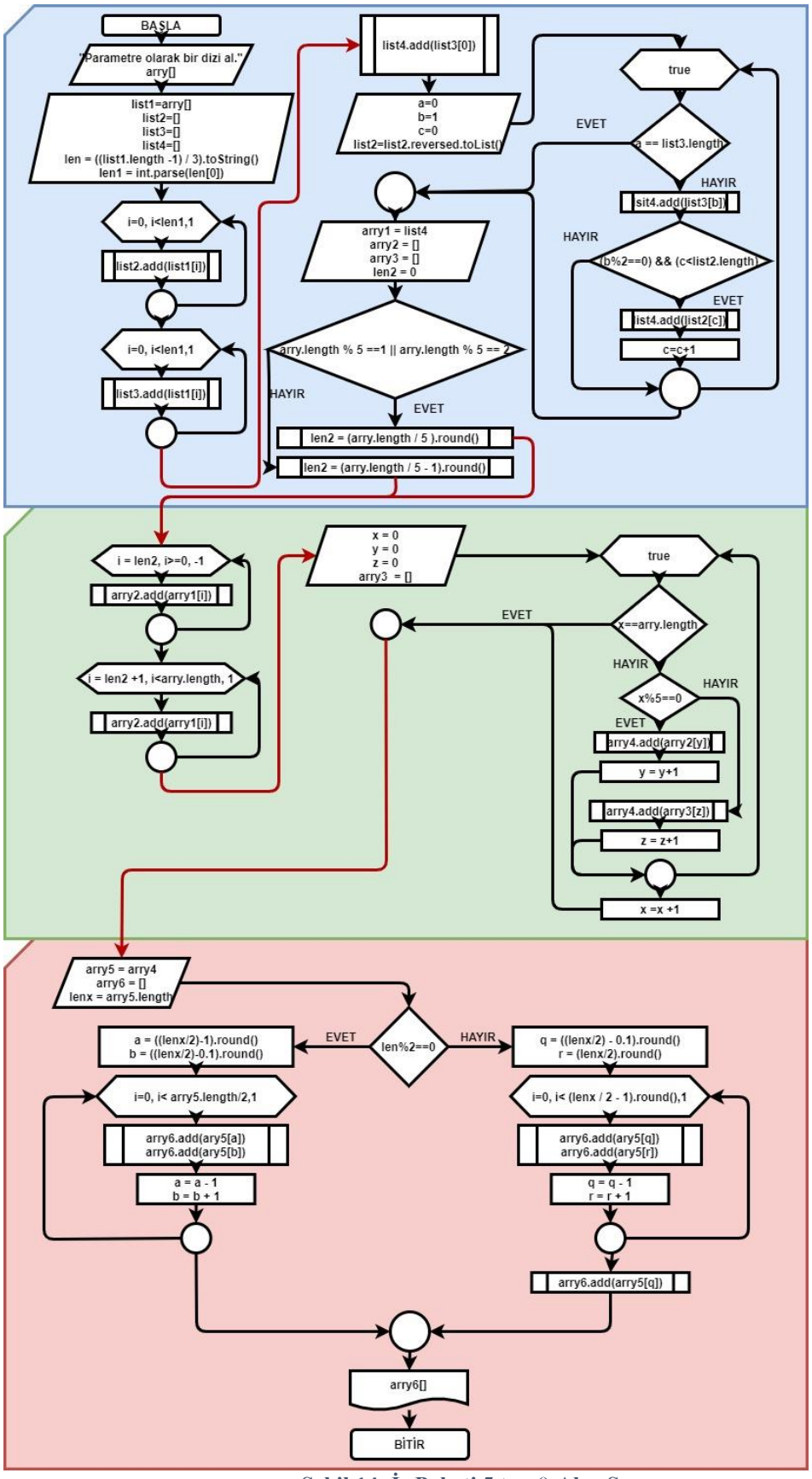
Şekil 12- İş Paketi 5 byteConversion() Akış Şeması

1.4.1.6 zigzag() Akış Şeması



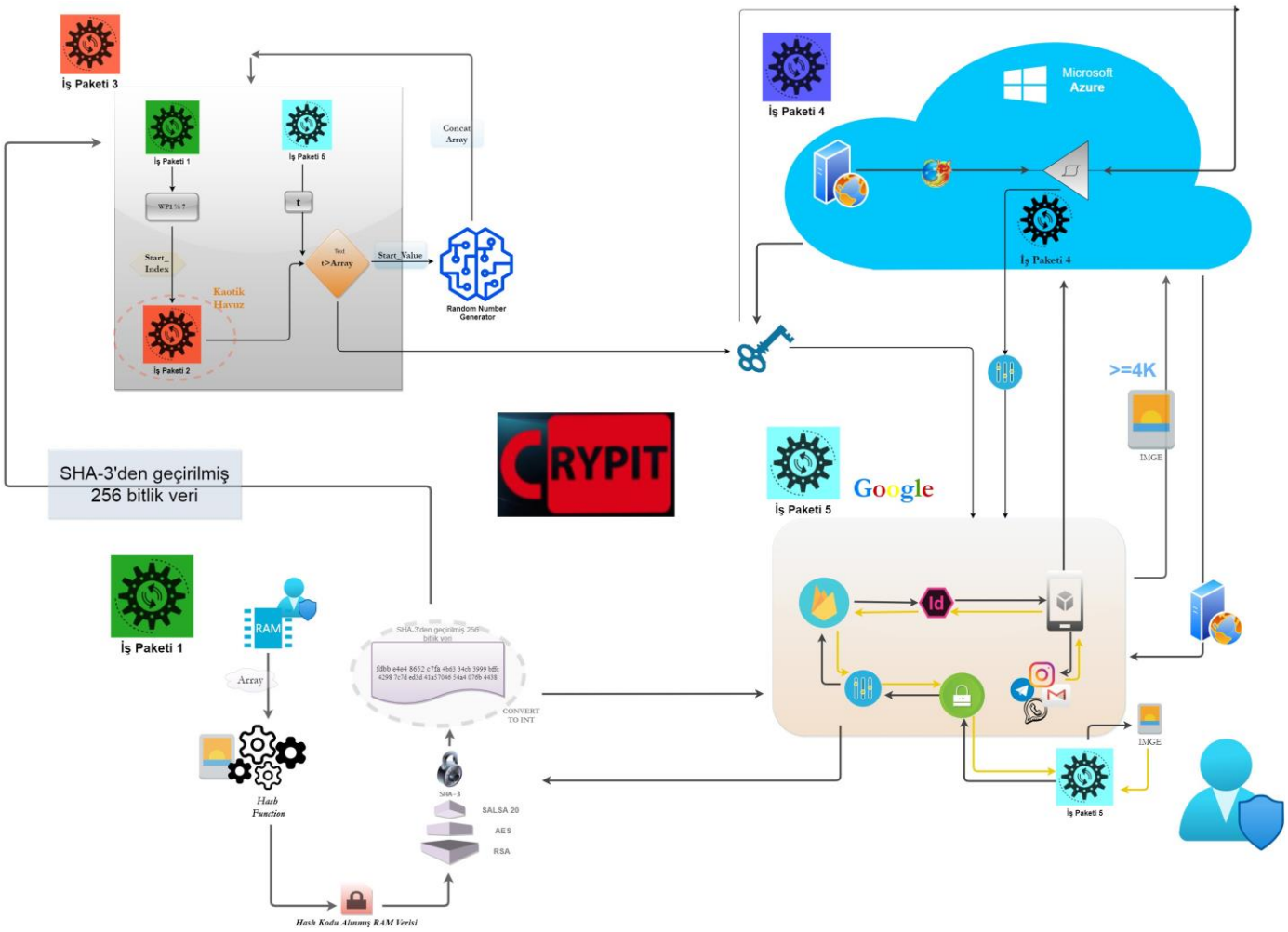
Şekil 13- İş Paketi 5 zigzag() Akış Şeması

1.4.1.7 ters(arry) Akış Şeması



Şekil 14- İş Paketi 5 ters() Akış Şeması

2 GERÇEKLEŞTİRİLEN SİSTEMİN GENEL MİMARİSİ



Şekil 15- Gerçekleştirilen Sistemin Genel Mimarisi