

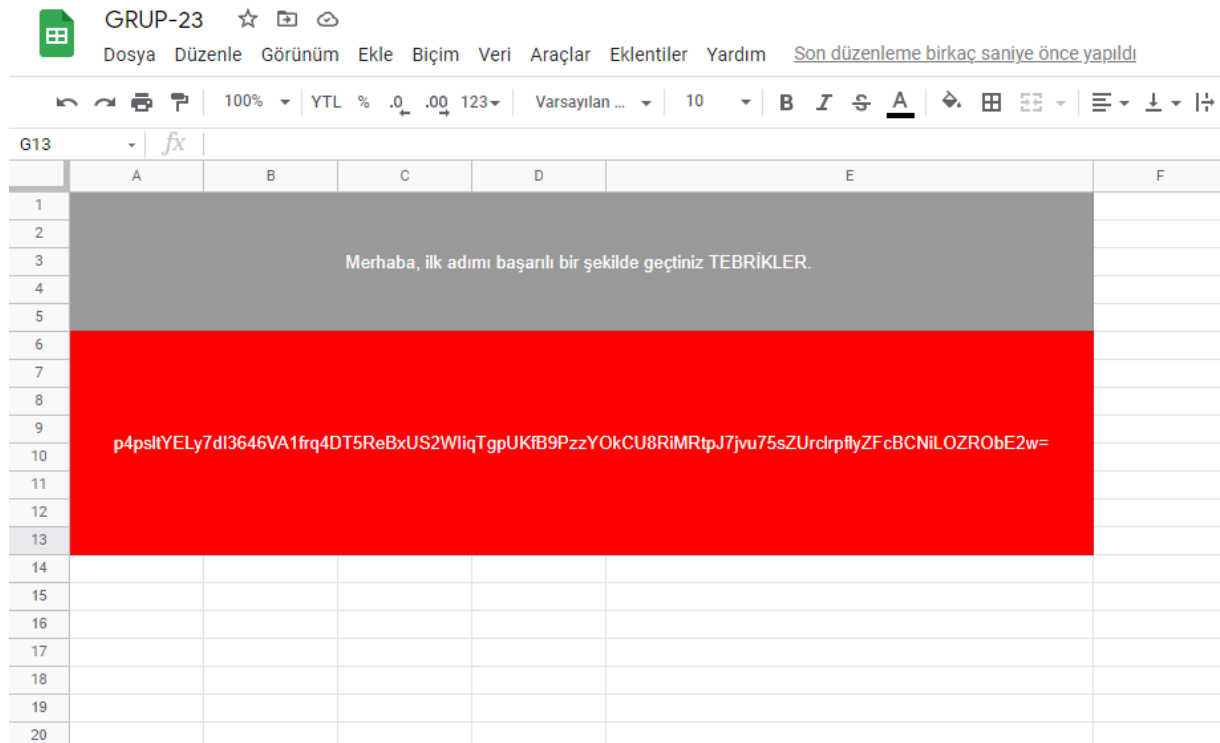
Hafta 2 LAB Uygulaması:

Her grup AES algoritmasını istediği programlama dilinde konsolda çalışacak halde ders günü hazır bulunacaktır.

1. Her grup 1 bilgisayar kullanacaktır.(Kendi bilgisayarları veya lab bilgisayarı tercih edilebilir.)
2. Bilgisayarlarda internet bağlantısı olmalıdır.

Yarışma formatında olacak haftada;

- Her gruba farklı şifrelenmiş metinler verilecektir.
- Gruplar detayları aşağıda belirtilen parametrelere göre verilen şifreli metinleri çözmesi beklenmektedir.
- Şifrelenmiş metinleri çözebilen gruplar daha önceden tarafımızca her grup için ayrı olarak tanımlanmış E-tablo linkine ulaşacaktır.
- Elde edilen linke herhangi bir tarayıcı yardımıyla bağlanan grupları aşağıdaki gibi bir tablo karşılayacaktır.



The screenshot shows a Google Sheet titled "GRUP-23". The sheet has a menu bar with options like "Dosya", "Düzenle", "Görünüm", "Ekle", "Biçim", "Veri", "Araçlar", "Eklentiler", and "Yardım". Below the menu bar is a toolbar with various icons for editing and formatting. The sheet itself has a grid with columns labeled A through F and rows numbered 1 through 20. In row 3, column A, there is a message: "Merhaba, ilk adımı başarılı bir şekilde geçtiniz TEBRİKLER." Below this message, from row 6 to row 13, there is a large red rectangular area. Inside this red area, in row 10, column A, there is a base64 encoded string: "p4psltYELy7dl3646VA1frq4DT5ReBxUS2WliqTgpUKfB9PzzYOkCU8RIMRtpJ7jvu75sZUrcrlpflyZFcBCNiLOZRObE2w=".

	A	B	C	D	E	F
1						
2						
3	Merhaba, ilk adımı başarılı bir şekilde geçtiniz TEBRİKLER.					
4						
5						
6						
7						
8						
9						
10	p4psltYELy7dl3646VA1frq4DT5ReBxUS2WliqTgpUKfB9PzzYOkCU8RIMRtpJ7jvu75sZUrcrlpflyZFcBCNiLOZRObE2w=					
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

- Kırmızı arka plana sahip şifrelenmiş metin tablo içerisinde yapmanız gereken görevi belirtmektedir.
- İlgili şifrelenmiş metni çözümleyip, belirtilen hücreye istenilen değeri girmeniz gerekmektedir.
- Fakat ilgili hücreye belirtilen değeri girerken açık text olarak değil de AES algoritmasıyla aynı parametreleri kullanarak şifrelenmiş halini girmeniz gerekmektedir.
- Görevini tamamlayan gruplar tabloyu kaydedip oturumu sonlandıracaktır.

AES Parametreleri:

32 bytes key

16 bytes Initialization vector

Text Format **Base64**

Mode: **CFB**

Türkçe karakter verilmeyecektir .

AES için yararlı linkler:

<https://pycryptodome.readthedocs.io/en/latest/src/cipher/aes.html>

<https://tr.wikipedia.org/wiki/AES>

<http://www.facweb.iitkgp.ac.in/~sourav/AES.pdf>

Algoritmanızı ders öncesinde denemeniz için örnekler:

1) Key = rnop3TnHwJ7P9zzLb0Z3qUjfhulCx9bW

iv = YsiebTh0Sjr8dZKo

Text Format **Base64**

Mode: **CFB**

Çözülmesi istenen şifreli metin :

p4psltayVQ7eTjVEfXVhJh2KML3BCeHj8eJz7OvWjpNVLbwsqDeIp492KHNqlD54w/FTTFL
IYxb4ABTEZfCj3r7uT4PDWWZMjhQ=

Ulaşılması gereken açık text :

Grup uyelerinin okul numaralarini virgul ile ayirarak G6 hucresine
girisiniz

2) Key = wEgDCNvhccofPTkFt9zUdDgZDIVdGC9L

iv = crGTopEfBGXE1klx

Text Format **Base64**

Mode: **CFB**

Çözülmesi istenen şifreli metin :

40YLp07vJIuR0TfMaNBvWwXdtsp5YFy56MU37H8=

Ulaşılması gereken açık text :

<http://yaz.tf.firat.edu.tr/tr>