

T.C.
MİLLİ EĞİTİM BAKANLIĞI
TEKNOPARK İSTANBUL MESLEKİ VE
TEKNİK ANADOLU LİSESİ

Milli İstihbarat Teşkilatının Yayınladığı Kriptoloji
Sorularının Uygulamalı Çözümleri

Haziran 2024

İSTANBUL

Giriş

Milli İstihbarat Teşkilatı, 21 Mayıs 2024'te resmi internet sitesi¹ üzerinden kriptoloji soruları yayınladı.

Sorular, farklı şifreleme algoritmaları kullanarak ele alınmaktadır. Siber güvenlik temalı yarışmalarda kriptoloji kapsamında sorular eksiksiz yer alır. Teknopark İstanbul MTAL olarak 2018'den bugüne düzenlediğimiz "Liseler Arası Bayrağı Yakala Yarışması"nda kriptoloji çerçevesinde sunduğumuz vakalar bulunmaktadır.

Güvenliğin temel taşlarından olan ve olmazsa olmazı konumundaki şifre bilimi, her siber güvenlik ilgisinin ve tabii öğrencilerimizin edinmesi gereken bir beceridir. Bu doğrultuda Teşkilat'ın yayınladığı sorular doğrudan odağımıza girmektedir.

Bu çalışmada, kriptolojinin siber güvenlikteki yerine kısaca değindikten sonra yayınlanan soruları tek tek analiz edip çözüme giden yolu aşamalı olarak ele alacağız.

¹ [www.mit.gov.tr/duyuru lorem-ipsum 42.html](http://www.mit.gov.tr/duyuru-lorem-ipsum-42.html)

Kriptolojinin Siber Güvenlikteki Yeri

Haberleşmenin gizliliğini sağlamak bireysel ve kamusal bir ihtiyaç olarak insanoğlunun gereksinimlerinden biridir.

Günümüzdeki teknolojik gelişmeler doğrultusunda ise şifre bilimi oldukça geniş bir sahada kıymetlendirilmektedir. Örneğin verileri şifrelemek için kullanılan AES ve RSA gibi algoritmalar hassas düzeydeki verileri şifrelemek ya da yetkisiz erişime karşı korumak için kullanılmaktadır. Yanı sıra güvenli iletişim de yine kriptoloji aracılığıyla yapılagelmektedir. Yaygın olarak kullanılan SSL/TLS, SSH ve IPSec gibi şifreleme protokolleri ağ güvenliğinde önemli yer tutmaktadırlar. Gittikçe yaygınlaşan dijital imzaların temeli de şifre biliminin geldiği noktaya dayanmaktadır. İlgili belge ve işlemlerin bütünlüğünü ve doğruluğunu sağlamasının yanı sıra süreçlerin pratikliğine olan katkısı ise başka bir yararlı yönüdür. Güncel bir teknoloji olarak blockchain ise özellikle merkezi olmayan sistemlerde işlem doğrulama ve veri bütünlüğüne katkı sağlamaktadır. Blockchain'in etkin çalışabilmesinin arkasındaki şifre bilimi, söz konusu yapının güvenilirliğini de sağlamaktadır.

Bilişim sistemleri olsun olmasın kriptoloji, güvenli iletişimin temel bir taşı olarak karşımızda durmaktadır. Siber güvenlik öğrencisinin bu yetiyle kendini donatmasında yarar görünmektedir.

Kriptolojinin Bayrağı Yakala Yarışmalarındaki Yeri

Bayrağı Yakala Yarışmaları -yaygın kullanımıyla Capture the Flag- siber güvenlik alanında bireylerin kendini geliştirebilecekleri bir tür öğretici oyunlardır. Ülkemizin ilk ve tek siber güvenlik lisesi olarak 2018'den bugüne ortaokul ve liseler arası bayrağı yakala yarışmaları düzenlemekteyiz. Bu yarışmalarda ise kriptoloji, alandaki ağırlığından dolayı soru havuzumuzdaki haklı yerini almaktadır.

Kriptoloji, CTF senaryolarında/sorularında şifreleme, şifre çözme, steganografi gibi çeşitli teknikler yoluyla kendini gösterir.

Yarışmacılar, hassas bilgilerin güvenliğini sağlamak, iletişim yollarını korumak ve rakiplerin verilere müdahale etme veya verileri değiştirme girişimlerini engellemek için kriptoloji tekniklerden yararlanabilir. Aynı zamanda saldırganlar da savunmaları aşmak, gizli verileri çıkarmak ve sistemlere yetkisiz erişim sağlamak için kriptanalizden yararlanabilir. Dolayısıyla CTF mücadelelerinde etkili bir savunma/saldırı için kriptolojinin incelikli bir şekilde anlaşılması temel bir koşuldur.

İlgili öğrencilerin bu ve benzer kriptoloji sorularını çözerek bakış açılarını zenginleştirmeleri olasıdır. Ulusal ve uluslararası bayrağı yakala yarışmalarına hazırlık için çözümleri okumak da güzel bir edinim yöntemidir.

1. soru

İlk soruda "CEZES NĖNS LIÜ ES LIÜ ÇIÜHI" ifadesi ve anahtar sayısının da 5 olarak seçildiđi bilgisi verilmektedir. Caesar, bilindiđi üzere harf kaydırma yöntemiyle veri gizlemeyi sağlar. Bilinen ve en eski şifreleme yöntemlerinden biridir. Günümüzde Caesar ile veri şifrelemesi pek tercih edilmese de kriptolojinin bilinen ilklerinden olduđu için temel bir bilgi olarak yerini korumaktadır.

Caesar'da var olan harfi 5 harf sonrasına ya da öncesine kaydırarak veri okunaklı biçime getirilebilmektedir. Türk alfabesine göre C'den beş önce gelen harf V olmaktadır. Benzer işlem adımı diđer harfler için de tek tek yapıldığında şifrelenmiş metnin açık biçimi ortaya çıkmaktadır. Elbette, otomatize olarak da bu işlem yaptırılabilirdi.

"CEZES NĖNS LIÜ ES LIÜ ÇIÜHI" ifadesinin açık olarak ulaşıldığı söz, MİT'in web sayfasında da yer alan söylemidir:

"VATAN İÇİN HER AN HER YERDE"

2. soru

İkinci soruya baktığımızda ise yeniden Caesar kullanıldığı görülmektedir. Bu kez açık metnin Caesar ile şifrelenmesi beklenmektedir. 1. sorudaki işlemin tersini yaparak şifreleme işlemi başarıyla gerçekleştirilebilir. Anahtarın 3 olarak belirtildiğini temel alırsak $M \rightarrow \underline{\text{Ö}} / E \rightarrow \underline{\text{Ğ}}...$

Caesar şifrelemesi elle yapılabildiği gibi çevrim içi hacking araçları da bu işlemi pek hızlı biçimde yapabilmektedir. Buradaki amacın şifreleme yönteminin nasıl yapıldığının farkındalığına kavuşturmak olduğunu var sayarsak otomatize araçlardan önce elle -manuel olarak-yapabilirliğini incelemekte yarar var. Nasıl şifrelendiğini ve çözülebildiğini bildikten sonra otomatize araçlara başvurmak doğru bir seçim olabilir.

Soruda çoktan seçmeli yanıtlar sıralanmaktadır:

- a) ÖĞTHDÇD
- b) PHUKDED
- c) JCOFVYV
- d) ABAHREM
- e) ÖĞTJÇDÇ

3. soru

Üçüncü soruda Route tekniği kullanılarak şifrelenmiş bir metin verilmektedir: "AİRERXXEDRANNVATÇEHEYNHİ". Yanı sıra yatay uzunluk biriminin 4 seçildiği ve saat yönünde spiral olarak şifrelendiği bilgisi de vurgulanmaktadır. Bu metnin açık halini bulmamız beklenmektedir. Ve bir not düşülmüştür: "X eksik kalan harfler yerine kullanılmıştır." Yöntemi bilmiyor olsak da hızlı bir araştırmayla bir yaklaşım geliştirilebilir. Doğru soru sormanın ve problem tanımlama yapmanın, çözümün ilk aşaması olduğu akılda tutulmalıdır.

Soruda uzunluk biriminin 4 olduğu belirtilmektedir. Verilen şifreli metin ise 24 harften oluşmaktadır: 24/4 işleme göre 6 satırlık bir tabloya göre yerleşim yapılması uygun olacaktır. Peki, sütun sayısı? Soruda yatay uzunluğu 4 verilmişti.

Öncelikle verilen metni dörderli olarak sıralayalım:

AİRE

RXXE

DRAN

NVAT

ÇEHE

YNHİ

Şimdi bu dörtlü satırları sağ üstten başlayarak tablodaki hücrelere yerleştirmemiz gerekiyor. Peki, neden sağ üstten yerleştiriyoruz? Açık metin Route ile şifrelenirken seçilen

4. soru

Dördüncü soruda, önceki ilk üç soruda olduğu gibi ayrıntılı bir bilgi verilmediği göze çarpmaktadır. Soru, olduğu gibi şu şekildedir:

Şifreli metinde hangi mesaj gizli?

“MÇİRY İİNEE TNHHR VAEND ATRAE”

İlk bakışta Caesar şifrelemesi gibi görünmektedir. Fakat soru içeriğinde herhangi bir anahtar sayısı belirtilmediği için bu olasılık devre dışı kalmaktadır. Caesar’da genellikle 3 ya da 5 sayısı anahtar olarak seçilir. Bu uygulandığında anlamlı bir sonuca ulaşamamıştır. Öyleyse nasıl yaklaşmalıdır? Bu aşamada bir bulmaca çözer gibi verilen sıralı harflere dikkat kesilebilir.

Bir deneme-yanılma yaklaşımıyla beş ayrı öbekten oluşan ifadenin baş harfleri üzerinden girildiğinde “M İ T V A...” ilerleyişi doğru bir iz üstünde olduğumuzun ipucunu vermiş oldu. Fakat ikinci harflere geçince benzer akıcılıkta sonuca varılamadı. Böylesi akla gelen ilk çözüm olabileceğinden burada takılmak olasıdır. Peki, ikinci kez başa dönmektense varış yerinden tersi yöne gidilse? Şimdi oldu gibi!

“MİT VATAN İÇİN HER AN HER YERDE”

5. soru

Beşinci ve son soruyu çözmek için dördüncü soruyu da çözebilmiş olmak gerektiği belirtilmektedir. Soru şöyledir:

Dördüncü sorunun cevabı ve verilen tablo ile senin için Atatürk'ün bir sözünü şifreledik. Bulabilir misin?

ÖDOPÇEARREJNSĞKTHJÇIUFINPŞIUNJEPVÖGÖMUUSPJZÖYC
ÇYNRĞJNTHUSÜIJFFNĞÖAOÖSAİLEKHUIÜNCUPPBSÖNTLSH
ÇÖÖRÜİDDBMLAYAYLTIOÖRNDTPRBJUEDYĞHELTAÖFĞRBEJ
TBUDPZIJVZVİÖÜPCŞOSNNHMŞTFJİUACOOISESKSUMÇÜLBZ
OBMÇFKZVÇÇZCÖÖĞSİCSTLÜ

A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L
L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M
M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K
K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N
N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J
J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O
O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ
İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö
Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I
I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P
P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H
H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R
R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ
Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S
S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G
G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş
Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F
F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T
T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E
E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U
U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D
D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü
Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç
Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V
V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C
C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B	Y
Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z	B
B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A	Z
Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	I	Ö	İ	O	J	N	K	M	L	A

Tablo 3: Soruda verilen tablo.

Dördüncü soruda olduğu gibi verilenleri inceleyip bir anlamlı bir yaklaşım yakalamaya çalışması gereken bir soruyla karşı karşıyayız gibi duruyor. Sol üstten gözlemlediğimizde alfabenin ilk harfi ile son harfi yan yana. Üçüncü sıradaki harf ise alfabemizdeki ikinci harf olurken dördüncü sıradaki harf ise yirmi sekizinci harfe denk geliyor. Birinci sütunun yukarıdan aşağıya doğru bakıldığında ise ilk satırın tersindeki harflerin sıralandığı da gözlem sonucu elde edilen unsurlar arasında. Bu bilgiler bir işe yarabilir mi? Dursun bakalım. Çözümüne giden tek bir yol yoktur nitekim.

Herhangi bir şifre bilimi soru içerisinde alfabetik bir tablo görüldüğünde akla Vigenere gelebilir. Caesar şifreleme üzerine kurulu bir şifreleme yöntemi olan Vigenere ile şifrelendiğini bilmek yararlı olabilir. Vigenere'in kendine has tablosu çeşitleri bulunmaktadır ancak burada bize özellikle bir tablo verildiği için referansımız buradaki olacaktır.

Dördüncü sorunun yanıtını bulmuştuk: "MİT VATAN İÇİN HER AN HER YERDE" idi. Elde ettiğimiz bu çıktıyı anahtar olarak kullanacağız. Öncesinde verilen tabloyu çözüme uygun biçime getirmemiz gerekmektedir. Tablonun sol ve üst kısımlarına Türk alfabesini yerleştirerek okumayı hızlandırmak olasıdır. Sütunda dördüncü sorunun yanıtı, satırda ise şifreli metnin baş harflerini sırasıyla temel alacağız.

ABCÇDEFGĞHI İJKLMNOÖPRŞŞTUÜVYZ

A	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L
B	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M
Ç	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K
D	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N
E	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J
F	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O
G	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ
H	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö
Ğ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ
H	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P
İ	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H
İ	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R
J	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ
K	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S
L	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G
M	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F
N	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E	T
O	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U	E
P	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D	U
P	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü	D
R	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç	Ü
R	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V	Ç
S	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C	V
S	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B	Y	C
T	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z	B
T	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A	Z
U	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
U	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
V	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
V	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
Y	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
Y	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A
Z	Z	B	Y	C	V	Ç	Ü	D	U	E	T	F	Ş	G	S	Ğ	R	H	P	İ	Ö	İ	O	J	N	K	M	L	A

Tablo 4: Kesişim noktalarına göre harflerin tespit edilmesi.

Bu aşamadan sonra sütun ve satırlardaki harflerin kesişimiyle şifreli metin açık hale getirilebilir (noktalar ve boşluklar okumada kolaylık olması adına eklenmiştir). Soruda şifrelenmiş olarak verilen metin çözüldüğünde Başöğretmenimiz Atatürk'ün o sözüne ulaşılır:

**“KÜÇÜK HANIMLAR KÜÇÜK BEYLER SİZLER HEPİNİZ
GELECEĞİN BİR GÜLÜ YILDIZI VE İKBAL İŞİĞİSİNİZ.
MEMLEKETİ ASIL İŞİĞA BOĞACAK OLAN SİZSİNİZ.
KENDİNİZİN NE KADAR ÖNEMLİ DEĞERLİ OLDUĞUNUZU
DÜŞÜNEREK ONA GÖRE ÇALIŞINIZ.
SİZLERDEN ÇOK ŞEY BEKLİYORUZ.”**

Sonuç

Teşkilat'ın çevrim içi ortamda yayınladığı kriptoloji soruları 2024 yılının başından bu yana MİT'in ortaya koymuş olduğu yeni nesil kamu diplomasisinin günceldeki bir çıktısı olarak değerlendirilebilir. Nitekim "Temas İstanbul" sergisi, 23 Nisan'da öğrencilere yönelik düzenlenen resim ve yazı etkinliği, Sn. Başkan'ın 23 Nisan Ulusal Egemenlik ve Çocuk Bayramı'nda çocuklara; 19 Mayıs Atatürk'ü Anma, Gençlik ve Spor Bayramı'nda ise gençlere yönelik yayınladığı mektupları bu stratejinin etkin ve görünür örnekleri arasında anılabilir.

Milli İstihbarat Teşkilatının toplumla aracısız, doğrudan iletişim kurma stratejisinin bir çıktısı olarak görülebilecek kriptoloji soruları kapsamındaki bu etkinlik aynı zamanda istihbarat servisi ile korumakla görevli olduğu ulusun arasındaki iletişimin sağlıklı biçimde kurulmasında etkin bir yöntem olduğu söylenebilir. Nitekim istihbarat, yaygın kanının aksine kaçınılması ve uzak durulması gereken bir alandan ötede zeka üzerine kurulu entelektüel bir faaliyettir.

Kriptoloji sorularının çeşitli zorluklarla yayınlanması ve kapsamının etkinliklerle desteklenmesi alana olan ilginin ve yetkinliğin artışında etkili olacağı düşünülmektedir.