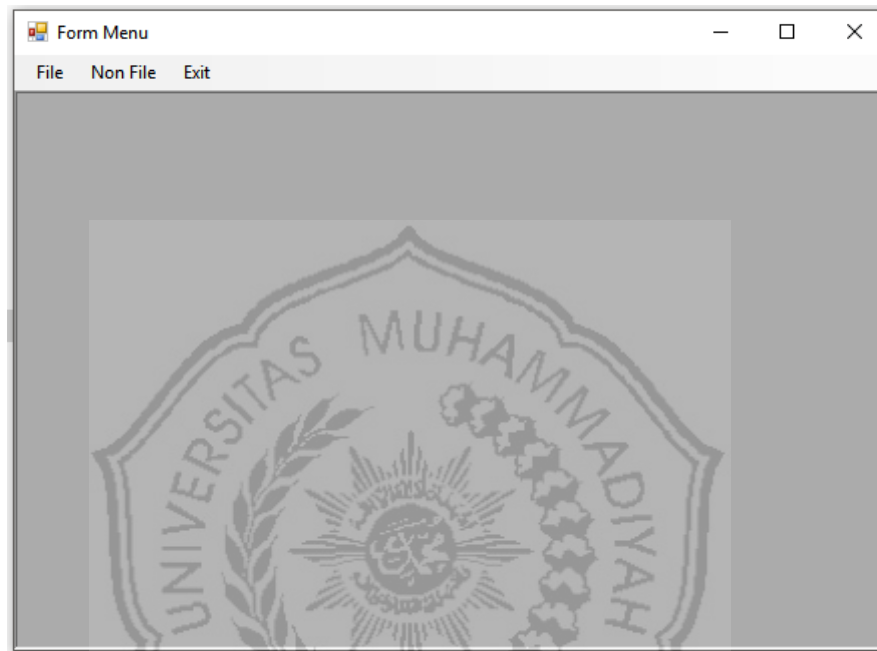


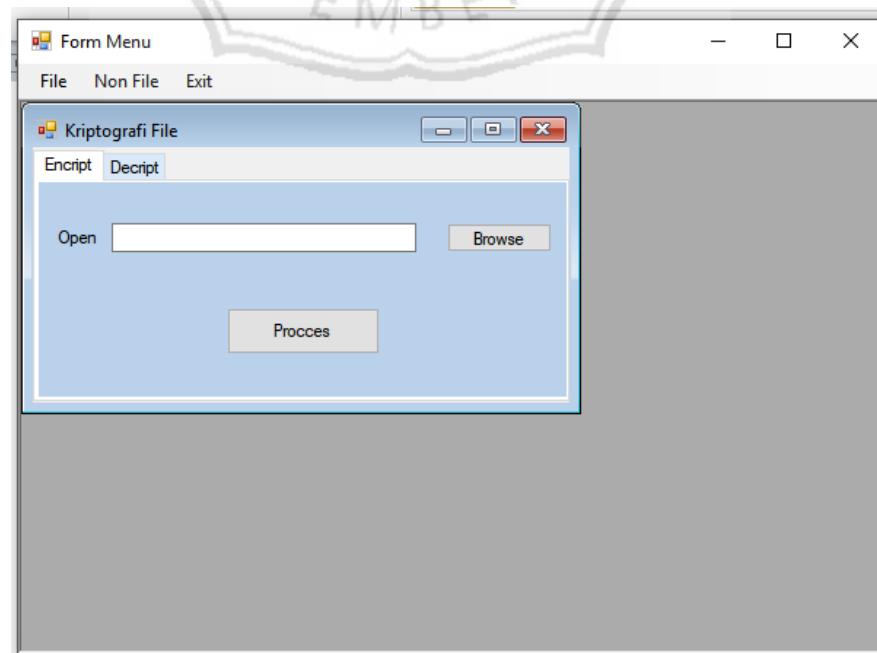
LAMPIRAN : Program Aplikasi

1. Desain Aplikasi

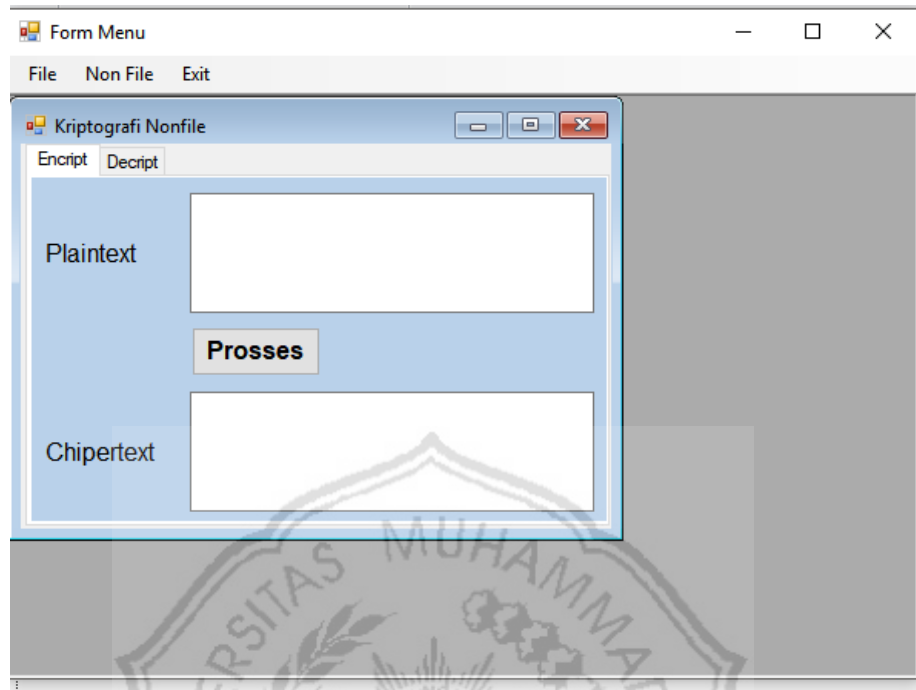
1.1 Tampilan Awal – Tampilan pembuka



1.2 Tampilan Menu File



1.3 Tampilan Menu Non-File



1.4 Coding Tampilan Awal

```
Public Class frmmenu

    Private Sub ExitToolStripMenuItem_Click(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles ExitToolStripMenuItem.Click
        Me.Close()
    End Sub

    Private Sub FileToolStripMenuItem_Click(ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles FileToolStripMenuItem.Click
        If frmnonfile.IsHandleCreated = True Then
            frmnonfile.Close()
        End If
        frmfile.MdiParent = Me
        frmfile.Show()
    End Sub

    Private Sub NonFileToolStripMenuItem_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
NonFileToolStripMenuItem.Click
        If frmfile.IsHandleCreated = True Then
            frmfile.Close()
        End If
        frmnonfile.MdiParent = Me
        frmnonfile.Show()
    End Sub

    Private Sub frmmenu_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
```

```

        Me.Text = "Form Menu"
    End Sub
End Class

```

1.5 Coding Menu File

```

Imports Microsoft.Office.Interop
Public Class frmfile

    Dim plaintext, chipertext As String
    Dim asci, dpn, blk As Integer
    Dim ext() As String
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button1.Click
        Dim open As Integer = OpenFileDialog1.ShowDialog()
        If open = vbCancel Then
            Exit Sub
        End If
        TextBox1.Text = OpenFileDialog1.FileName
    End Sub

    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button2.Click
        chipertext = ""
        ext = Split(TextBox1.Text, ".")
        If TextBox1.Text <> "" Then
            Select Case ext(ext.Length - 1)
                Case "txt"
                    Dim teks As New System.IO.StreamReader(TextBox1.Text)
                    plaintext = teks.ReadToEnd
                Case "doc", "docx"
                    Dim objWord As New Word.Application
                    Dim objDoc As Word.Document
                    objDoc = objWord.Documents.Open(TextBox1.Text)
                    For i = 1 To objWord.ActiveDocument.Paragraphs.Count
                        objWord.ActiveDocument.Paragraphs(i).Range.Select()
                        plaintext +=
objWord.ActiveDocument.Paragraphs(i).Range.Text
                    Next
                    objDoc.Close()
                    objWord.Quit()
                End Select
            End If
            _encrip()
            _simpan(1)
        End Sub

    Private Sub Button4_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button4.Click
        Dim open As Integer = OpenFileDialog1.ShowDialog()
        If open = vbCancel Then
            Exit Sub
        End If
        Dim teks As New System.IO.StreamReader(OpenFileDialog1.FileName)
        chipertext = teks.ReadToEnd

```

```

        TextBox2.Text = OpenFileDialog1.FileName
    End Sub

    Private Sub Button3_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button3.Click
        plaintext = ""
        _decrip()
        _simpan(2)
    End Sub

    Private Sub _simpan(ByVal sm As Integer)
        Dim open As Integer = SaveFileDialog1.ShowDialog()
        If open = vbCancel Then
            Exit Sub
        End If
        '
        If sm = 1 Then
            If System.IO.File.Exists(SaveFileDialog1.FileName & ".dll") =
True Then
                My.Computer.FileSystem.DeleteFile(SaveFileDialog1.FileName
& ".dll")
            End If
            System.IO.File.WriteAllText(SaveFileDialog1.FileName & ".dll",
chipertext)
        Else
            If System.IO.File.Exists(SaveFileDialog1.FileName & ".txt") =
True Then
                My.Computer.FileSystem.DeleteFile(SaveFileDialog1.FileName
& ".txt")
            End If
            System.IO.File.WriteAllText(SaveFileDialog1.FileName & ".txt",
plaintext)
        End If
    End Sub

    Public Sub _encrip()
        chipertext = ""
        Dim rd As Double
        Dim tks As String
        For i = 1 To plaintext.Length
            asci = Asc(GetChar(plaintext, i))
            rd = asci / 30
            tks = GetChar(rd.ToString, 1)
            dpn = Convert.ToInt32(tks)
            blk = (asci Mod 30) + 1

            If chipertext = "" Then
                chipertext = Chr(dpn) + Chr(blk)
            Else
                chipertext += Chr(dpn) + Chr(blk)
            End If
        Next
    End Sub

    Public Sub _decrip()
        plaintext = ""

```

```

For i = 1 To chipertext.Length
    If i Mod 2 = 0 Then
        blk = Asc(GetChar(chipertext, i))

        asci = (dpn * 30) + blk - 1
        If plaintext = "" Then
            plaintext = Chr(asci).ToString
        Else
            plaintext += Chr(asci).ToString
        End If
    Else
        dpn = Asc(GetChar(chipertext, i))
    End If
Next
End Sub

Private Sub frmfile_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
    Me.Text = "Kriptografi File"
End Sub
End Class

```

1.6 Tampilan Menu Non-File

```

Public Class frmnonfile

    Dim plaintext, chipertext As String
    Dim asci, dpn, blk As Integer

    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button2.Click
        chipertext = ""
        plaintext = ""
        chipertext = TextBox4.Text
        _decrip()
        TextBox3.Text = plaintext
    End Sub

    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button1.Click
        chipertext = ""
        plaintext = ""
        plaintext = TextBox1.Text
        _encrip()
        TextBox2.Text = chipertext
    End Sub

    Public Sub _encrip()
        chipertext = ""
        Dim rd As Double
        Dim tks As String
        For i = 1 To plaintext.Length
            asci = Asc(GetChar(plaintext, i))
            rd = asci / 30
            tks = GetChar(rd.ToString, 1)
            dpn = Convert.ToInt32(tks)
            blk = (asci Mod 30) + 1

```

```

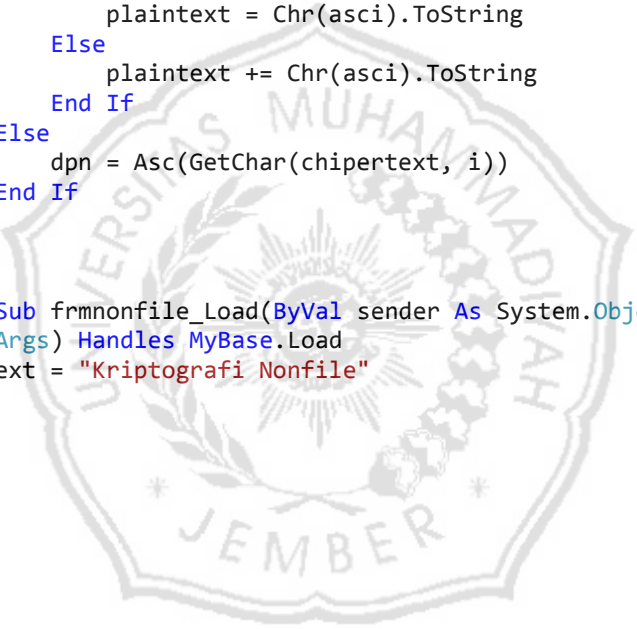
        If chipertext = "" Then
            chipertext = Chr(dpn) + Chr(blk)
        Else
            chipertext += Chr(dpn) + Chr(blk)
        End If
    Next
End Sub

Public Sub _decrip()
    plaintext = ""
    For i = 1 To chipertext.Length
        If i Mod 2 = 0 Then
            blk = Asc(GetChar(chipertext, i))

            asci = (dpn * 30) + blk - 1
            If plaintext = "" Then
                plaintext = Chr(asci).ToString
            Else
                plaintext += Chr(asci).ToString
            End If
        Else
            dpn = Asc(GetChar(chipertext, i))
        End If
    Next
End Sub

Private Sub frmnonfile_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
    Me.Text = "Kriptografi Nonfile"
End Sub
End Class

```



LAMPIRAN : ASCII CODE

Tabel ASCII

The ASCII code

American Standard Code for Information Interchange

www.theasciicode.com.ar

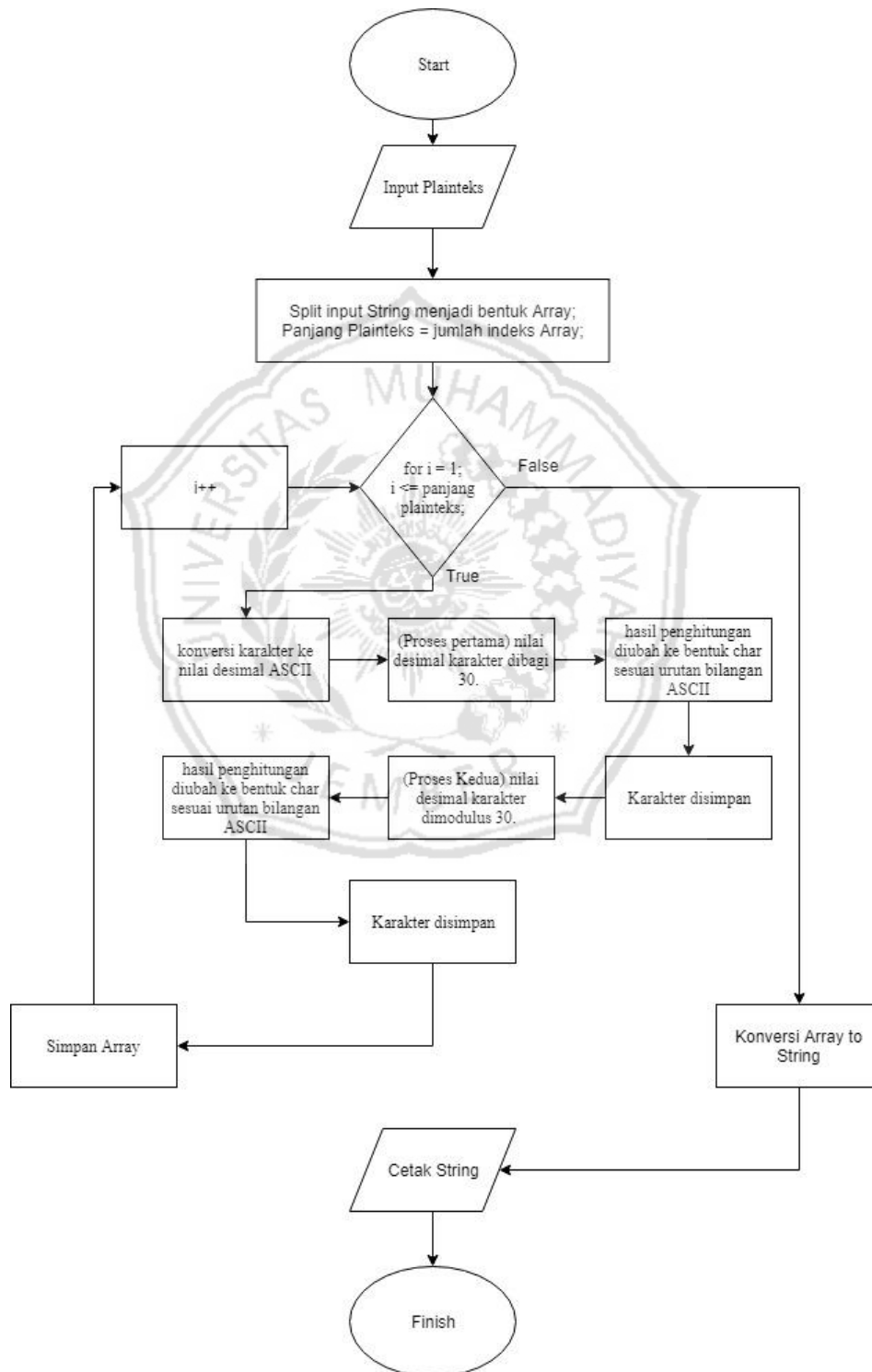
ASCII control characters		ASCII printable characters						Extended ASCII characters								
DEC	HEX	Simbolo	Simbolo	Simbolo	Simbolo	Simbolo	Simbolo	DEC	HEX	Simbolo	Simbolo	Simbolo	Simbolo	Simbolo	Simbolo	
00	00h	NULL	(carácter nulo)	32	20h	espacio	64	40h	@	96	60h	.	128	80h	Ç	
01	01h	SOH	(inicio encabezado)	33	21h	!	65	41h	A	97	61h	a	129	81h	Ù	
02	02h	STX	(inicio texto)	34	22h	"	66	42h	B	98	62h	b	130	82h	É	
03	03h	ETX	(fin de texto)	35	23h	#	67	43h	C	99	63h	c	131	83h	À	
04	04h	EOT	(fin transmisión)	36	24h	\$	68	44h	D	100	64h	d	132	84h	Á	
05	05h	ENQ	(enquiry)	37	25h	%	69	45h	E	101	65h	e	133	85h	Â	
06	06h	ACK	(acknowledgement)	38	26h	&	70	46h	F	102	66h	f	134	86h	Ã	
07	07h	BEL	(timbre)	39	27h	'	71	47h	G	103	67h	g	135	87h	Ä	
08	08h	BS	(retroceso)	40	28h	(72	48h	H	104	68h	h	136	88h	Å	
09	09h	HT	(tab horizontal)	41	29h)	73	49h	I	105	69h	i	137	89h	Æ	
10	0Ah	LF	(salto de línea)	42	2Ah	*	74	4Ah	J	106	6Ah	j	138	8Ah	È	
11	0Bh	VT	(tab vertical)	43	2Bh	+	75	4Bh	K	107	6Bh	k	139	8Bh	Ë	
12	0Ch	FF	(form feed)	44	2Ch	,	76	4Ch	L	108	6Ch	l	140	8Ch	Ì	
13	0Dh	CR	(retorno de carro)	45	2Dh	-	77	4Dh	M	109	6Dh	m	141	8Dh	Í	
14	0Eh	SO	(shift Out)	46	2Eh	=	78	4Eh	N	110	6Eh	n	142	8Eh	Î	
15	0Fh	SI	(shift In)	47	2Fh	/	79	4Fh	O	111	6Fh	o	143	8Fh	Ï	
16	10h	DLE	(data link escape)	48	30h	0	80	50h	P	112	70h	p	144	90h	Ï	
17	11h	DC1	(device control 1)	49	31h	1	81	51h	Q	113	71h	q	145	91h	Ï	
18	12h	DC2	(device control 2)	50	32h	2	82	52h	R	114	72h	r	146	92h	Ï	
19	13h	DC3	(device control 3)	51	33h	3	83	53h	S	115	73h	s	147	93h	Ï	
20	14h	DC4	(device control 4)	52	34h	4	84	54h	T	116	74h	t	148	94h	Ï	
21	15h	NAK	(negative acknowle.)	53	35h	5	85	55h	U	117	75h	u	149	95h	Ï	
22	16h	SYN	(synchronous idle)	54	36h	6	86	56h	V	118	76h	v	150	96h	Ï	
23	17h	ETB	(end of trans. block)	55	37h	7	87	57h	W	119	77h	w	151	97h	Ï	
24	18h	CAN	(cancel)	56	38h	8	88	58h	X	120	78h	x	152	98h	Ï	
25	19h	EM	(end of medium)	57	39h	9	89	59h	Y	121	79h	y	153	99h	Ï	
26	1Ah	SUB	(substitute)	58	3Ah	:	90	5Ah	Z	122	7Ah	z	154	9Ah	Ï	
27	1Bh	ESC	(escape)	59	3Bh	;	91	5Bh	[123	7Bh	{	155	9Bh	Ï	
28	1Ch	FS	(file separator)	60	3Ch	<	92	5Ch	\	124	7Ch		156	9Ch	Ï	
29	1Dh	GS	(group separator)	61	3Dh	=	93	5Dh]	125	7Dh	}	157	9Dh	Ï	
30	1Eh	RS	(record separator)	62	3Eh	>	94	5Eh	^	126	7Eh	~	158	9Eh	Ï	
31	1Fh	US	(unit separator)	63	3Fh	?	95	5Fh	_				159	9Fh	f	
127	20h	DEL	(delete)													

Di akses pada hari selasa, tanggal 12 Maret 2019 di :

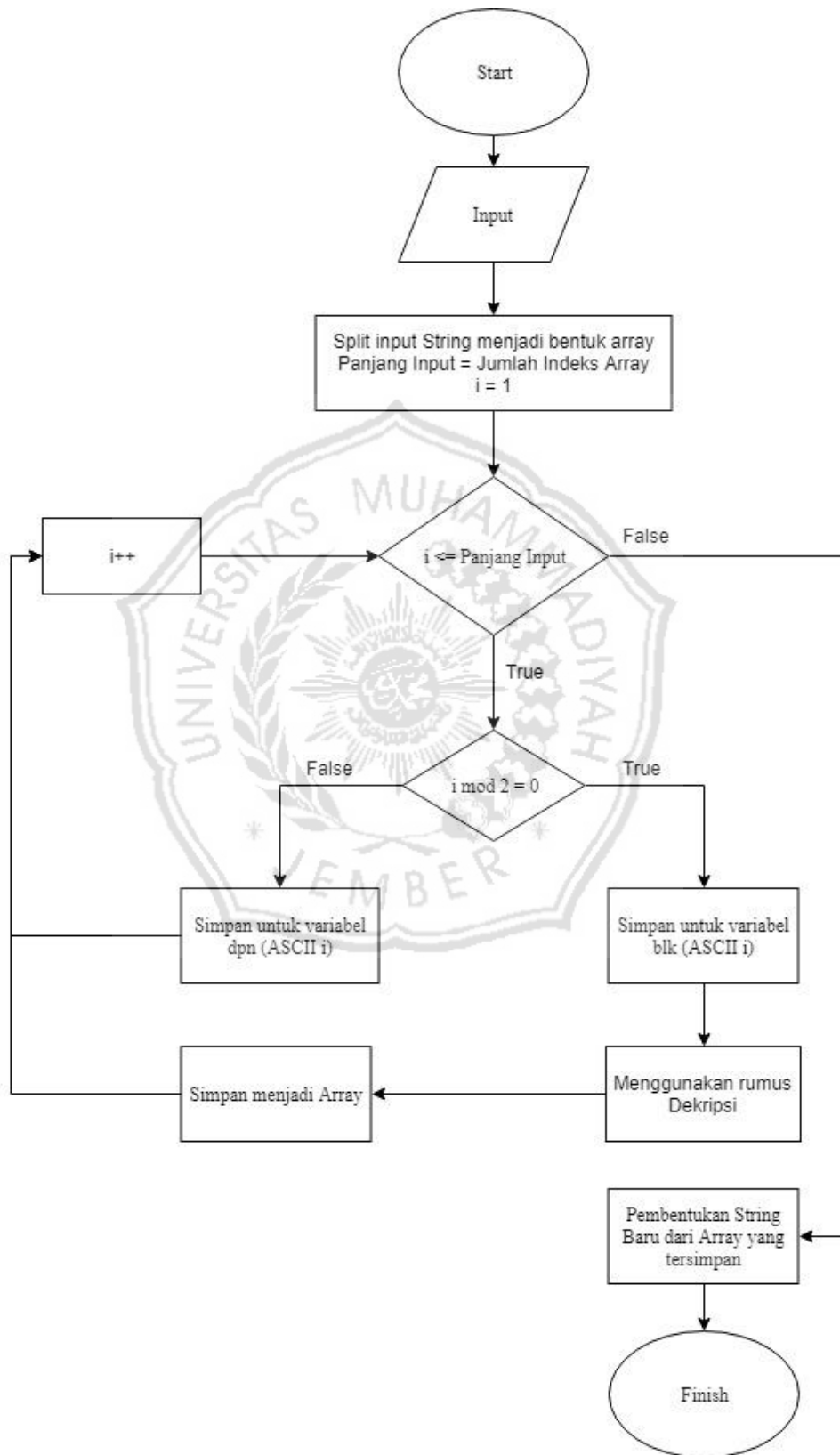
<http://silent-detective.blogspot.com/2012/09/ascii-american-standard-code-for.html>

LAMPIRAN : DIAGRAM ALUR PROSES ENKRIPSI DAN DEKRIPSI

Diagram Alur Proses Enkripsi



2. Diagram Alur Proses Dekripsi



LAMPIRAN : FILE UJI

File 1 (Jumlah kata : 485; Kapasitas File : 15KB)

Bencana Banjir Kencong Timbulkan Empati Mahasiswa Internasional UM Jember

Duka atas kejadian bencana banjir yang terjadi di kota jember pada minggu 23 Desember 2018, akibat air penahan dinding Sungai Tanggul Jebol di Dusun KedungLangkap Kraton Kencong telah menimbulkan banyak simpati dari berbagai kalangan masyarakat untuk berusaha membantu meringankan beban para korban banjir, tak terkecuali juga sekelompok mahasiswa internasional UM Jember yang tergerak hatinya untuk ikut serta membantu meringankan beban korban bencana dengan jalan melakukan bakti sosial dengan mengumpulkan berbagai bahan bantuan untuk disumbangkan. Tepat pada tanggal 30 Desember 2018 lalu, sekelompok mahasiswa Internasional ini berangkat ke kencong dengan membawa barang barang bantuan. " kami dari mahasiswa Internasional negara thailand merasa sedih dan perihatin atas kejadian bencana banjir yang terjadi di kota jember, kami yang tinggal di indonesia khususnya kota jember sebagai pilihan kami untuk belajar merasa sangat penting bagi kami untuk membantu saudara kami yang sedang membutuhkan bantuan maka dengan ini kami merencanakan agenda bakti sosial ini sebagai bentuk rasa keprihatnan kami", jelas Nurulhuda Dueromae mahasiswa Thailand. "kami membawa barang bantuan seperti sembako, baju untuk semua usia, buku dan perlengkapan tulis, serta air mineral sebanyak 100 dus untuk para korban", imbuh Nurulhuda.

Rombongan yang berjumlah 38 orang yang terdiri dari mahasiswa thailand, timor leste dan malaysia ini berangkat pada pukul 13.00 WIB menuju lokasi dengan dipimpin oleh ibu Nurul Fathiyah F M.P selaku kepala KUI (Kantor Urusan Internasional) sekaligus sebagai ketua rombongan menuju posko muhammadiyah yang berada di desa igir-igir. Rombongan disambut oleh Farud AFA selaku kordinator relawan Muhammadiyah dari MDMC (muhammadiyah disaster management center).

Sesampainya di posko muhammadiyah para mahasiswa Internasional ini diberikan arahan terlebih dahulu oleh Farud AFA kordinator relawan muhammadiyah tentang lokasi yang akan dituju. Kelompok mahasiswa dibagi menjadi dua yang selanjutnya dibawa menggunakan mobil pick up terbuka menuju lokasi bencana membantu membagikan logistik kepada beberapa korban bencana dilokasi yang masih terendam banjir.

Farud AFA mengatakan bahwa daerah yang akan dituju adalah dusun Panggul melati desa Kepanjen kecamatan Gumukmas yang kondisinya masih terendam banjir sampai lutut serta masih dalam keadaan padam listrik.

Beberapa kegiatan yang dilakukan oleh mahasiswa Internasional ini selain membantu Distribusi Logistik berupa Sembako, Peralatan Bersih bersih, Peralatan Bayi dan Selimut mereka juga membantu untuk asament beberapa data yang dibutuhkan sesuai instruksi.

Nurul Fatiyah Fauzi selaku ketua rombongan juga menyampaikan bahwa seluruh hasil bantuan yang dibawa oleh mahasiswa asing ini adalah hasil dari kesukarelaan mereka dan komunitas mereka tanpa ada paksaan dan kegiatan bakti sosial ini juga atas inisiatif mereka dan rasa empati mereka secara pribadi dan kami membantu dalam hal fasilitas dan menghubungkan dengan pihak-pihak yang terkait.

"Saya pribadi berharap semoga apa yang kami lakukan dapat memberikan keringan dan banyam keberkahan untuk mereka, kami berdo'a semoga Tuhan memberikan keselamatan untuk mereka dan kita semua Amiin " ujar Vergilio Antonio Jose mahasiswa Timur Leste.

File 2 (Jumlah Kata : 411; Kapasitas File : 15KB)

Bencana Terjang 13 Desa di Jember, Satu Orang Dilaporkan Meninggal

Jember - Akibat hujan deras yang mengguyur Kabupaten Jember sejak hari Sabtu (23/12) sore hingga malam hari, tercatat ada 13 desa yang terdampak bencana. Selain menimbulkan kerusakan fisik, satu orang dilaporkan meninggal.

Berdasarkan laporan yang dihimpun dari Badan Penanggulangan Bencana Daerah (BPBD) Kabupaten Jember, bencana yang diakibatkan curah hujan tinggi tersebut di antaranya banjir, tanah longsor dan angin kencang di beberapa titik.

"Hujan intensitas sedang di beberapa wilayah Jember, menyebabkan bencana banjir, angin kencang dan tanah longsor di beberapa wilayah. Hingga saat ini masih dilakukan proses pendataan dampak dari bencana itu," ujar Kabid Kedaruratan dan Logistik BPBD Jember Heru Widagdo saat dikonfirmasi detikcom, Minggu (23/12/2018)

Untuk sementara diketahui ada satu korban meninggal dunia. Korban diketahui tersengat aliran listrik saat banjir merendam rumahnya.

"Atas nama Imam umur 42 tahun warga Desa Kaliwining, Kecamatan Rambipuji. Jenazah sudah disemayamkan dan pagi tadi dimakamkan," ungkap Heru.

Untuk mengatasi bencana tersebut, Heru mengatakan Pusdalops BPBD Jember telah berkomunikasi dengan jajaran samping.

"TRC BPBD berangkat ke lokasi kejadian untuk assessment dan membantu evakuasi warga terdampak. Sampai saat ini, proses pendataan juga masih dilakukan," tambahnya.

Sementara itu, Kapolres Jember AKBP Kusworo Wibowo menambahkan, pihaknya telah menerjunkan sejumlah personel untuk ambil bagian dalam penanggulangan bencana.

"Mulai tadi malam kita sudah terjun ke anggota ke titik-titik lokasi," tandasnya.

Selain itu, petugas juga melakukan pemantauan di sejumlah titik rawan timbulnya bencana. "Kita terus pantau untuk berjaga-jaga agar bisa cepat ikut dalam penanganan jika terjadi bencana," lanjutnya.

Berdasarkan data yang dihimpun BPBD Jember, berikut lokasi titik bencana yang terjadi di Kabupaten Jember.

1. Kecamatan Wuluhan
Desa Glundengan, Dusun Sumberejo dan Tanjungsari
Jumlah warga terdampak 492 KK
2. Kecamatan Balung
Desa Curah Lele, Dusun Karang Pakem, Krajan Tengah, dan Krajan Kidul
Jumlah warga terdampak 170 KK
3. Kecamatan Rambipuji
Desa Kaliwining
Satu orang meninggal dunia bernama Imam (42) akibat tersengat listrik saat banjir merendam rumahnya
4. Kecamatan Bangsalsari
Desa Sukorejo dan Petung
Jumlah warga terdampak 230 KK
5. Kecamatan Sumpalsari
Desa Pakem, banjir menggenangi jalan perumahan, jumlah warga terdampak masih dalam proses pendataan
6. Kecamatan Sumberbaru
Desa Kaliglagah dan Yosorati (Dalam proses pendataan); Desa Sumberagung, jumlah warga terdampak 400 KK
7. Kecamatan Tempurejo
Desa Sanenrejo dan Wonoasri (Dalam proses pendataan)
8. Kecamatan Kencong
Desa Keraton, Dusun Kedung Langkap (Dalam proses pendataan)
9. Kecamatan Gumukmas
Desa Sidomulyo (Dalam proses pendataan)
10. Kecamatan Ajung
Desa Pancakarya, Dusun Krasak
Jumlah warga terdampak 60 KK
11. Kecamatan Semboro
Desa Semboro, Dusun Semboro (Dalam proses pendataan)

Petani di Jember Dapat Kucuran KUR dari Perbankan

TRIBUNNEWS.COM, JEMBER - Kementerian Pertanian, Pemerintah Kabupaten [Jember](#), dan PT BNI Tbk memberikan dukungan kepada petani dalam mengelola dan mengembangkan pertanian.

Dukungan itu diwujudkan dengan memberikan Kredit Usaha Rakyat (KUR) untuk petani.

"Hari ini direalisasikan KUR untuk petani, dan ini baru pemanasan saja," kata Bupati [Jember](#) Faida dalam acara Mengawal Gerakan Musim Tanam Oktober - Maret 2018 - 2019 di Desa Jatisari Kecamatan Jenggawah, [Jember](#), Rabu (5/12/2018).

Kegiatan Mengawal Gerakan Musim Tanam, menurut bupati, menjadi bukti petani bisa mengakses layanan lembaga keuangan.

Karena itu, bupati berharap gerakan ini menjadi gerakan massal, sehingga petani lebih sejahtera dan perbankan bisa lebih bermanfaat bagi petani.

Selain memberikan kredit melalui KUR, BNI juga telah menyalurkan dana Corporate Social Responsibility (CSR) kepada petani untuk pembangunan saluran irigasi dengan kegiatan padat karya tunai yang melibatkan sekitar 200 orang petani.

Lebih jauh Bupati Faida menegaskan dukungan untuk program inklusi keuangan oleh perbankan, karena sudah ada di RPJMD (Rencana Pembangunan Jangka Menengah Daerah) [Jember](#).

Petani yang akses terhadap lembaga keuangan pasti lebih sejahtera. "Dan itu tidak banyak diketahui oleh petani. Jadi kita harus lebih dekat dengan mereka," ungkap bupati.

Inklusi keuangan untuk pertanian akan diluaskan lagi, seperti untuk pupuk. Dan sudah waktunya meninggalkan cara-cara lama atau cara cash," tegasnya.

Faida kemudian menegaskan, petani jaman now sudah waktunya memakai sistem pembayaran non tunai.

"Petani juga berhak mengikuti kemajuan teknologi dan kemajuan pelayanan lembaga keuangan," lanjutnya.

Untuk pengembangan pertanian, Pemerintah Kabupaten [Jember](#) akan menyiapkan lahan tambahan. Selain itu, pemerintah daerah akan memberi bantuan bibit serta pelatihan pertanian.

Sementara itu, Direktur Pupuk dan Pestisida Kementerian Pertanian RI Muhrizal Sarwani menyampaikan, kegiatan ini merupakan contoh dari sinergitas antara pemerintah pusat dan daerah.

"Kita dorong penggunaan Kartu Tani ini, yang di dalamnya ada KUR," kata Muhrizal.

KUR itu untuk sekitar 1 hektar lahan pertanian dengan uang kurang lebih Rp. 14 juta. Kartu ini juga bisa untuk membeli pupuk. Pembelian pupuk di kios pupuk sekarang non cash atau menggunakan kartu tani.

GM Divisi Bisnis usaha kecil BNI Bambang Setyatmojo mengatakan KUR BNI di [Jember](#) sudah hampir Rp 15 miliar, yang disalurkan kepada 1400 petani. Di Kecamatan Jenggawah sudah lebih dari 40 petani.

"Dari 40 tani ini bisa menularkan bahwa dari BNI ada kemudahan akses. Bunganya ringan dan bayarnya ketika panen," katanya.

Bambang mengatakan, bantuan dan pelatihan dari BNI akan disinergikan dengan Pemkab [Jember](#) dan Kementerian Pertanian.

Artikel ini telah tayang di [Tribunnews.com](#) dengan judul Petani di Jember Dapat Kucuran KUR dari

Perbankan, <http://www.tribunnews.com/regional/2018/12/05/petani-di-jember-dapat-kucuran-kur-dari-perbankan>.

Editor: Sugiyarto

File 4 (Jumlah Kata : 372; Kapasitas File : 15KB)

UM Jember Terapkan Model Bimbingan Terpadu Untuk Mahasiswa KKN 2019, di Kota Jember

Program KKN 2019 telah resmi dibuka. Rektor Universitas Muhammadiyah Jember Dr Ir M Hazmi DESS., secara resmi membuka acara pembekalan KKN di Aula Zaenuri pada Selasa 15/01/2019 kemarin. Kuliah Kerja Nyata (KKN) lahir dalam proses pembangunan yang pada hakekatnya adalah pelaksanaan dari falsafah pendidikan yang berdasarkan pada Undang-undang Dasar 1945 dan Undang-undang nomor 22 tahun 1961, dalam pengalaman Tridharma Perguruan Tinggi.

Pada tahun 2019 ini UM Jember akan menerjunkan 894 Mahasiswa KKN yang terdiri dari 8 Fakultas diantaranya Fakultas Hukum, FKIP, Fakultas Ekonomi, FIKES, Psikologi, Pertanian, Teknik FISIPOL dan FAI beberapa kecamatan di kabupaten jember diantaranya Balung, Bangsalsari, Kencong, Jombang, Semboro, dan Gumukmas. Total desa yang akan menjadi tempat para mahasiswa KKN ini sebanyak 43 Desa.

Menurut Dr. Nurul Qomariyah M.M mengatakan bahwa KKN 2019 membawa tema Taman Bacaan Masyarakat dengan memadukan sebuah studi Etnografi. Studi Etnografi yang artinya Filed Work yakni turun langsung mencari data ke lapangan, untuk menemukan, kemudian menggambarkan, secara holistic, sistem sosiokultural suatu masyarakat atau cara hidup suatu masyarakat. Etnografi adalah hidup bersama masyarakat, melihat kehidupan sehari-hari mereka, bergaul dengan mereka, mendengar pembicaraan mereka, berbual dalam bahasa mereka dan melihat dunia sebagaimana mereka melihatnya. Dengan demikian studi ini diharapkan mampu mendorong setiap Mahasiswa agar bekerja di Desa dalam rangka pengabdian dalam jangka waktu tertentu untuk tinggal dan bekerjasama membantu masyarakat pedesaan dalam mengerjakan persoalan pembangunan”
Jelas Dr. Nurul Qomariyah M.M selaku kepala LPPM. “ manfaat lain mahasiswa dapat mengembangkan pemikiran berdasarkan ilmu teknologi dan dalam upaya menumbuhkan, mempercepat serta mempersiapkan kader-kader pembangunan”,
Imbuhnya. KKN akan dilaksanakan pada 31 Januari-1 Maret 2019 mendatang.
Menurut Dhian Wahana Pura M.Pd.I selaku dosen pembimbing KKN mengatakan

dalam KKN ini akan memberikan instruksi kepada mahasiswa agar menanamkan minat baca kepada masyarakat, mengingat menambah wawasan atau pengetahuan selain sebagai perintah agama juga merupakan media membuka cakrawala. dalam proses membimbing mahasiswa KKN Dhian Wahana Pura M.Pd.I memaparkan bahwa akan melakukan model bimbingan “terpadu” yang artinya pembimbing akan membimbing satu kesatuan agar mereka mampu menguasai banyak antara kemampuan berinteraksi dimasyarakat, moral di masyarakat, menunjukkan intelektual movement di masyarakat serta religious dimasyarakat. Dengan demikian output tujuan KKN akan tercapai meliputi masyarakat sadar literasi, masyarakat berfikir cerdas dan mahasiswa dapat membawa nilai promotif terhadap lembaga dimasyarakat.

File 5 (Jumlah Kata : 265; Kapasitas File : 14KB)

Kabupaten Bandung - Ferdi Firmansyah (13), Lucky Parikesit (13) dan Agip Trisakti (15) ditemukan tewas di Gunung Tampomas, Sumedang, Jabar. Ketiga pendaki itu diduga tewas akibat mengalami hipotermia.

Keberadaan ketiga remaja yang ditemukan dengan terbujur kaku di dalam tenda itu pertama kali diketahui pendaki lainnya, Minggu (3/3). Saksi lalu melaporkannya kepada pos pendakian.

Tim SAR gabungan lalu dikerahkan untuk mengevakuasi para korban asal Indramayu tersebut. Saat ditemukan, ketiga korban dalam posisi meringkuk seperti menahan kedinginan di Pos 4 Gunung Tampomas.

"Dugaan sementara karena hipotermia. Saat ditemukan tubuh para korban seperti meringkuk menahan dingin," kata Humas dan Protokoler Basarnas Kantor SAR Bandung, Joshua Banjarnahor kepada wartawan.

Ketiga korban ditemukan dalam kondisi pakaian yang basah akibat hujan. Tidak ditemukan pakaian ganti atau jaket dalam barang bawaan ketiganya. Identitas juga luput dari barang bawaan ketiganya.

Menurut Joshua, kondisi pakaian yang basah membuat ketiganya sangat mungkin mengalami hipotermia. Apalagi, saat itu angin di Gunung Tampomas cukup kencang.

"Mereka ala kadarnya pakai kaos dan celana. Gak bawa pakaian ganti, jaket atau sleeping bag," ungkap dia.

Tim SAR mengevakuasi jasad ketiganya menggunakan kantong jenazah dan tandu kayu dari puncak gunung. Jenazah ketiganya lalu dibawa ke RSUD Sumedang untuk ditindaklanjuti pihak kepolisian.

Kapolres Indramayu AKBP M. Yoris mengatakan ketiganya merupakan warga Blok Kuang BTM, Desa Tugu Kidul, Kecamatan Sliyeg, Indramayu. Mereka berangkat dari rumahnya masing-masing menuju Gunung Tampomas, pada Sabtu (2/3) pukul 06.00 WIB.

"Mereka pergi menggunakan satu unit motor Nopol E 5560 PAV," kata Yoris kepada detikcom, Minggu (3/3)

Pihak keluarga sudah menjemput para korban dari RSUD Sumedang untuk dibawa ke rumah duka di Indramayu."Sudah dijemput pihak keluarga," kata Yoris.
(mud/ern)

File 6 (Jumlah Kata : 332; Kapasitas File : 16KB)

Kriptografi (atau kriptologi; dari bahasa Yunani [κρυπτός](#) *kryptós*, "tersembunyi, rahasia"; dan [γράφειν](#) *graphein*, "menulis", atau [λογία](#) *logi*, "ilmu")^[1] atau sandisastra merupakan keahlian dan ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga.^[2] Secara umum, kriptografi ialah mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan;^[3] berbagai aspek dalam [keamanan informasi](#) seperti data rahasia, [integritas data](#), [otentikasi](#), dan [non-repudansi](#)^[4] merupakan pusat dari kriptografi modern. Kriptografi modern terjadi karena terdapat titik temu antara disiplin ilmu [matematika](#), [ilmu komputer](#), dan [teknik elektro](#). Aplikasi dari kriptografi termasuk [ATM](#), [password komputer](#), dan [E-commerce](#).

Kriptografi sebelum merupakan sinonim dari "[enkripsi](#)", konversi dari kalimat-kalimat yang dapat dibaca menjadi kelihatan tidak masuk akal. Pembuat dari pesan enkripsi membagi teknik pemecahan sandi yang dibutuhkan untuk mengembalikan informasi asli jika hanya dengan penerima yang diinginkan, sehingga dapat mencegah orang yang tidak diinginkan melakukan hal yang sama. Sejak [Perang Dunia I](#) dan kedatangan [komputer](#), metode yang digunakan untuk mengelola kriptologi telah meningkat secara kompleks dan pengaplikasiannya telah tersebar luar.

Kriptografi modern sangat didasari pada teori matematis dan aplikasi komputer; algoritme kriptografi didesain pada asumsi ketahanan komputasional, membuat algoritme ini sangat sulit dipecahkan oleh musuh. Secara teoretis, sangat sulit memecahkan sistem kriptografi, namun tidak layak melakukannya dengan cara-cara praktis. Skema ini oleh karena itu disebut sangat aman secara komputasional; kemajuan teoretis dapat meningkatkan algoritme faktorisasi integer, dan meningkatkan teknologi komputasi yang membutuhkan solusi ini untuk diadaptasi terus-menerus. Terdapat skema keamanan informasi yang benar-benar tidak boleh dapat ditembus bahkan dengan komputasi yang tak terbatas namun skema ini sangat sulit diimplementasikan.

Teknologi yang berhubungan dengan kriptologi memiliki banyak masalah legal.

Di Inggris, penambahan Regulasi Penyelidikan Aksi Wewenang membutuhkan kriminal yang tertuduh harus menyerahkan kunci dekripsinya jika diminta oleh penegah hukum. Jika tidak pengguna akan menghadapi hukum pidana.[\[5\]](#) [Electronic Frontier Foundation](#) (EFF) terlibat dalam sebuah kasus di Amerika Serikat yang mempertanyakan jika seorang tersangka harus untuk menyerahkan kunci dekripsi mereka kepada pengak hukum merupakan inkonstitusionil. EFF memperdebatkan bahwa regulasi ini merupakan pelanggaran hak untuk tidak dipaksa mencurigai dirinya sendiri, seperti dalam Amendemen Kelima Konsitusi Amerika.[\[6\]](#)

File 7 (Jumlah Kata : 504; Kapasitas File : 16KB)

Kriptanalisis dari alat mekanis baru terbukti lebih sulit dan melelahkan. Di Inggris, usaha kriptanalisis di Bletchley Park selama Perang Dunia II memacu perkembangan alat yang lebih efisien untuk membawa tugas yang berulang-ulang. Hal ini berujung pada pengembangan Colossus, komputer digital pertama sekali yang bekerja penuh secara elektronik, yang membantu penyandi untuk mendekripsikan mesin Lorenz SZ40/42 milik tentara Jerman. Seperti juga pengembangan komputer digital dan elektronik, kriptanalisis juga berkembang menjadi lebih kompleks. Lebih jauh lagi, komputer dapat mengenkripsi setiap jenis data yang mungkin dalam bentuk biner, tidak seperti chiper klasik yang hanya mengenkripsi teks bahasa tertulis; hal ini sangat baru dan signifikan. Penggunaan komputer telah menggantikan kriptografi bahasa, baik untuk desain chiper dan kriptanalisis. Banyak chiper komputer dapat dikategorikan dengan operasi mereka pada urutan biner (kadang dalam grup atau blok), tidak seperti skema mekanikal dan klasik, yang biasa memanipulasikan karakter tradisional (seperti surat dan digit) secara langsung. Bagaimanapun, komputer juga membantu kriptanalisis, yang mengimbangi hingga batas tertentu untuk kompleksitas chiper yang lebih tinggi. Namun, chiper modern yang baik telah mengungguli kriptanalisis; kasus ini biasa menggunakan kualitas chiper yang lebih efisien (seperti membutuhkan sumber daya yang sedikit dan cepat, seperti memori atau kapabilitas CPU), sedang mendekripsikannya membutuhkan usaha dengan urutan yang lebih besar, dan lebih luas dibandingkan chiper yang lebih klasik, membuat kriptanalisis menjadi lebih tidak efisien dan tidak berguna. Riset akademik kriptografi yang terbuka luas masih relatif baru; dimulai pada pertengahan 1970an. Pada saat ini, personel IBM mendesain algoritme yang menjadi standar enkripsi data Federal; Whitfield Diffie dan Martin Hellman mempublikasikan algoritme perjanjian mereka.[\[17\]](#) dan algoritme RSA yang dipublikasikan oleh kolumnis Amerika Martin Gardner. Sejak saat itu, kriptografi telah sangat luas digunakan dalam dunia komunikasi, jaringan komputer, dan keamanan komputer secara umum. Beberapa teknik kriptografi modern dapat menyimpan kunci rahasianya jika menggunakan masalah matematika rumit, seperti faktorisasi integer atau masalah logaritma diskrit, jadi terdapat hubungan yang mendalam dengan matematika abstrak. Tidak ada bukti pasti bahwa teknik kriptografi aman. Saat terbaik, terdapat bukti bahwa beberapa teknik

aman jika beberapa masalah komputasional sulit untuk dipecahkan, atau asumsi tertentu mengenai implementasi atau penggunaan praktis bertemu.

Semakin mengetahui sejarah kriptografi, algoritme kriptografi dan desainer sistem harus juga bijaksana mempertimbangkan pengembangan masa depan saat bekerja dengan desain mereka. Sebagai contoh, pengembangan kontinu pada computer processing power telah meningkatkan cakupan brute-force attack, jadi ketika menentukan panjang kunci, diharuskan memilih kunci yang sulit.[18] Efek potensial dari komputer kuantum telah dipertimbangkan oleh beberapa sistem desainer kriptografi; implementasi kecil dari mesin ini yang akan segera diumumkan mungkin akan membutuhkan perhatian khusus ketimbang hanya spekulatif.[4]

Pada Dasarnya, pada awal abad ke-20, kriptografi secara singkat berkenaan dengan [bahasa](#) dan pola lexicographic. Sejak saat itu tekanannya telah berubah, dan kriptografi saat ini lebih luas menggunakan matematika, termasuk aspek [teori informasi](#), [kompleksitas komputasional](#), [statistik](#), [kombinasi](#), [aljabar](#), [teori bilangan](#), dan matematika diskrit secara umum. Kriptografi juga merupakan cabang [teknik](#), namun tidak biasa sebab hal ini berkaitan dengan pertentangan yang aktif, pintar, dan jahat; teknik jenis lain (seperti teknik kimia dan sipil) hanya membutuhkan gaya natural netral. Terdapat juga riset berkembang yang memeriksa hubungan antara masalah kriptografi dan [fisika kuantum](#).

File 8 (Jumlah Kata : 448; Kapasitas File : 16KB)

Kriptografi kunci-simetris merujuk pada metode enkripsi di mana kedua pengirim dan penerima membagi kunci yang sama (atau, walaupun kuncinya tidak mirip, namun dapat berhubungan dengan cara komputasi sederhana). Hal ini menjadi satu-satunya jenis enkripsi yang ketahu publik hingga Juni 1976.[17][[Berkas:International Data Encryption Algorithm InfoBox Diagram.svg|jmpl|Satu putaran (dari 8.5) chiper International Data Encryption Algorithm, digunakan pada beberapa versi PGP (Pretty Good Privacy) untuk enkripsi tingkat tinggi, seperti [e-mail](#) Chiper kunci simetris diimplementasikan baik itu sebagai chiper blok atau chiper stream. Sebuah block chiper enchiper masukan pada blok plainteks sebagai lawanan untuk karakter individual, bentuk masukan yang digunakan oleh chiper aliran.

Standar Enkripsi Data (SED) dan Standar Enkripsi Lanjutan (SEL) merupakan desain chiper blok yang telah ditunjuk sebagai standar kriptografi oleh pemerintah Amerika (walaupun penunjukan SED pada akhirnya ditarik setelah SEL diadopsi).[19] Walaupun penarikannya sebagai standar resmi, SED (masih menjadi varian yang masih terbukti dan lebih aman) masih cukup terkenal; Hal ini digunakan oleh banyak penerapan dari enkripsi ATM[20] hingga keamanan [e-mail](#)[21] dan akses remote aman.[22] Banyak chiper blok lainnya telah didesain dan dirilis, dengan kualitas yang bervariasi. Banyak telah juga yang dihancurkan, seperti FEAL[4][23]

Beberapa chiper, yang berbeda dengan tipe 'blok', membuat berkas panjang material kunci yang panjang, di mana dikombinasikan dengan bit-bit teks atau

karakter-karakter, sedikit mirip dengan one-time pad. Pada chiper aliran, aliran keluarannya diciptakan berdasarkan keadaan internal yang tersembunyi yang berubah saat chiper bekerja. Keadaan internal mulanya diatur menggunakan bahan kunci rahasia. RC4 sangat luas digunakan sebagai chiper aliran.[4] Chiper blok dapat digunakan sebagai chiper aliran.

Fungsi hash Kriptografi merupakan algoritme kriptografi tipe ke-tiga. Fungsi ini mengambil segala panjang pesan sebagai input, dan panjang keluaran hash yang pendek dan tetap, yang dapat digunakan sebagai (sebagai contoh) tanda tangan digital. Untuk memiliki fungsi hash yang baik, penyerang tidak dapat mencari dua pesan yang dapat menghasilkan hash yang sama. MD4 merupakan fungsi hash pangjang yang sekarang telah dapat dipecahkan; MD5, varian yang lebih kuat dari MD4, sudah luas digunakan namun dapat dipecahkan saat beroperasi. Agensi keamanan nasional Amerika mengembangkan serial Algoritme Hash Aman seperti fungsi hash MD5: SHA-0 ialah algoritme cacat yang kemudian ditarik; SHA-1 digunakan secara luas dan lebih aman dari MD5, namun kriptanalisis telah menemukan serangan padanya; keluarga SHA-2 meningkatkan performa SHA-1, namun belum secara luas digunakan; dan kewenangan Amerika mengatakan hal ini cukup bijaksana dari sudut pandang keamanan untuk mengembangkan standar baru "toolkit algoritme hash NIST secara keseluruhan untuk peningkatan kekuatan secara signifikan.[24] Sehingga, pada tahun 2012, standar nasional Amerika memilih SHA-3 sebagai standar desain hash yang baru.[25]

Message authentication code (MAC) hampir mirip dengan fungsi hash kriptografi, kecuali terdapat kunci rahasia yang dapat digunakan untuk membuktikan nilai hash melalui serangkaian resepep;[4] kerumitan tambahan yang melindungi skema serangan algoritme penyingkat sederhana, dan dianggap cukup menguntungkan.

File 9 (Jumlah Kata : 737; Kapasitas File : 17KB)

Kriptosistem kunci-simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi sebuah pesan, walaupun pesan atau kelompok pesan dapat memiliki kunci yang berbeda dari yang lain. Kerugian yang paling signifikan dari chiper simetris ialah kebutuhan manajerial kunci untuk menggunakannya secara aman. Setiap sepasang pihak komunikasi yang berbeda harus, idealnya, membagi kunci yang berbeda, dan juga membagi textchiper yang berbeda juga. jumlah kunci yang dibutuhkan meningkat dua kali lipat dari jumlah anggota jaringan, yang sangat cepat membutuhkan skema manajemen kunci komplek untuk menjaga semuanya tetap konsisten dan rahasia. Kesulitan dari menciptakan kunci rahasia yang aman di antara dua pihak yang saling berkomunikasi, ialah, ketika belum adanya jaringan aman di antara keduanya, juga kehadiran chicken-and-egg problem yang dianggap menjadi tantangan praktikal untuk pengguna kriptografi di dunia nyata.

[[Berkas:Diffie and Hellman.jpg|jmpl|kiri|Whitfield Diffie dan Martin Hellman, penulis jurnal pertama kriptografi kunci-publik]] Pada jurnal pionir tahun 1976, Whifiled Diffie dan Martin Hellman mengusulkan istilah dari kriptografikunci-

publik (juga, secara umum, disebut kunci asimetris) pada dua istilah yang berbeda namun secara matematis terdapat kunci yang berhubungan, yaitu kunci publik dan kunci privat.[26] Sistem kunci publik dikonstruksikan sangat baik sehingga kalkulasi dari satu kunci ('kunci privat') secara komputasional tidak mirip dengan (kunci 'publik') walaupun secara kebutuhan mereka mirip. Malah, kedua kunci dihasilkan secara rahasia, sebagai pasangan yang tidak berhubungan.[27] Sejarawan [David Kahn](#) menjelaskan kriptografi kunci-publik sebagai "konsep baru paling revolusioner dalam bidang ini sejak substitusi polialfabetik yang ditemukan pada masa Renaissance"[28]

Dalam ekosistem kunci-publik, kunci publik dapat secara bebas terdistribusi, saat pasangannya kunci privat harus selalu terjaga rahasia. Pada sistem enkripsi kunci-publik, kunci publik digunakan untuk enkripsi, sedang kunci privat atau rahasia digunakan untuk dekripsi. Sementara Diffie dan Hellman tidak dapat menemukan sistem seperti itu, mereka menunjukkan bahwa kriptografi kunci-publik memang benar mungkin dengan menunjukkan protokol [Diffie-Hellman key exchange](#), sebuah solusi yang sekarang digunakan secara luas dalam komunikasi aman, mengizinkan dua kelompok untuk secara rahasia membagi kunci enkripsi.[17]

Jurnal Diffie dan Hellman menyebar luas pada dunia akademi dalam mencari sistem enkripsi kunci-publik praktis. Lalu pada tahun 1978 [Ronald Rivest](#), [Adi Shamir](#), dan [Len Adleman](#), menemukan solusi yang kini dikenal sebagai [algoritme RSA](#). [29]

Algoritme Diffie-Hellman dan RSA, sebagai tambahan dalam menciptakan contoh algoritme kunci-publik kualitas tinggi pertama yang dikenal publik, telah sangat luas digunakan. Yang lain termasuk [Kriptosistem Cramer-Shoup](#), [Enkripsi ElGamal](#), dan varian [Teknik kurva eliptis](#).

Lalu, dokumen yang dipublikasikan pada tahun 1997 oleh Government Communication Headquarters (GCHQ), organisasi rahasia Inggris, mengungkapkan bahwa kriptografer di GCHQ telah mengantisipasi beberapa pengembangan akademik.[30] Dilaporkan, sekitar tahun 1970, [James H. Ellis](#) telah memahami prinsip kriptografi kunci asimetris. Pada tahun 1973, [Clifford Cocks](#) menemukan sulisi yang esensialnya menyerupai algoritme RSA.[30][31] Dan pada tahun 1974, [Malcom J. Williamson](#) diklaim telah mengembangkan algoritme pertukaran Diffie-Hellman.[32]

Kriptografi kunci-publik dapat juga digunakan untuk mengimplementasikan skema [tanda tangan digital](#). Tanda tangan digital berhubungan dengan tanda tangan pada umumnya; mereka memiliki karakteristik yang sama dimana mudah bagi pengguna untuk membuatnya, namun sangat sulit bagi orang lain untuk memalsukannya. Tanda tangan digital dapat juga secara permanen mengikat pada konten pesan yang sedang ditanda tangani; mereka lalu tidak dapat 'dipindahkan' dari satu dokumen ke dokumen yang lain, dan setiap usaha akan dapat terdeteksi. Pada skema tanda tangan digital, terdapat dua algoritme: satu untuk menandatangani, di mana kunci rahasia digunakan untuk memproses pesan (atau hash dari pesan, atau keduanya), dan satu untuk verifikasi, di mana kunci publik yang sesuai digunakan dengan pesan untuk memeriksa validitas tanda tangan. RSA dan DSA merupakan dua skema tanda tangan digital yang paling

terkenal. Tanda tangan digital merupakan pusat dari operasi infrastruktur kunci publik dan banyak skema keamanan jaringan lainnya (seperti [Transport Layer Security](#), [VPN](#), dll).[23]

Algoritme kunci publik paling sering didasari pada teori masalah kompleksitas komputasional, sering dengan [teori bilangan](#). Sebagai contoh, kekuatan RSA berhubungan dengan masalah [faktorisasi integer](#), sedangkan Diffie-Hellman dan DSA berhubungan dengan masalah [logaritma diskrit](#). Baru-baru saja, kriptografi kurva eliptis telah ditemukan, sistem di mana keamanan yang didasari pada masalah teoretis bilangan yang melibatkan kurva eliptis. Dikarenakan kesulitan masalah pokok, kebanyakan algoritme kunci-publik melibatkan operasi seperti eksponensial dan perkalian aritmetika modular, di mana teknik ini secara komputasional lebih mahal ketimbang teknik yang digunakan pada banyak chiper blok, khususnya dengan ukuran kunci yang dibutuhkan. Hasilnya, kriptosistem kunci-publik seringkali merupakan kriptosistem hybrid, yang merupakan algoritme enkripsi kunci-simetris berkualitas tinggi digunakan untuk pesan itu sendiri, sedang kunci simetris yang relevan dikirimkan dengan pesan, namun dienkripsikan menggunakan algoritme kunci publik. Hampir sama, skema tanda tangan hybrid sering digunakan, di mana fungsi hash kriptografi dihitung secara komputer, dan hanya hash hasil yang ditanda tangani secara digital.[4]

File 10 (Jumlah Kata : 3; Kapasitas File : 13KB)

Pengujian kalimat sederhana

File 11 (Jumlah Kata : 6; Kapasitas File : 13KB)

Pengujian kalimat lebih panjang dari sebelumnya

File 12 (Jumlah Kata : 15; Kapasitas File : 13KB)

Pengujian kalimat lebih kompleks menggunakan perpaduan numerik dan simbol – simbol 873 ^\$%() :>} {“:’>[];’)(*&^%\$ 4567.

File 13 (Jumlah Kata : 666; Kapasitas File : 16KB)

Tujuan dari kriptanalisis ialah untuk menemukan kelemahan dan ketidakamanan skema kriptografi, sehingga memungkinkan peningkatan atau perbaikan. Terdapat kesalahpahaman umum bahwa setiap metode enkripsi dapat dipecahkan. Hubungan dengan karya [Claude Shannon](#) di [Bell Labs](#) pada Perang Dunia II, membuktikan bahwa chiper one-time pad tidak dapat dipecahkan, menemukan kunci utama yang acak, tidak pernah dapat digunakan lagi, menyimpan rahasia dari setiap penyerang, dan memiliki panjang yang sama dan lebih besar dari pesan itu sendiri.[33] Kebanyakan chiper, selain one-time pad, dapat dipecahkan dengan

cara komputasional [brute force attack](#), namun jumlah usaha yang dibutuhkan dapat sangat lama tergantung pada besar kunci, sebanding dengan usaha yang dibutuhkan untuk membuat chipper. Pada beberapa kasus, keamanan yang efektif dapat dicapai jika terbukti bahwa usaha yang dibutuhkan (seperti "faktor kerja", dalam istilah Shannon) melebihi kemampuan dari setiap musuh. Ini berarti bahwa tidak boleh ada metode yang efisien (berbanding terbalik dengan metode brute force yang menghabiskan waktu) dapat ditemukan untuk memecahkan chipper. Sejak tidak ada bukti yang ditemukan, metode one-time-pad tetap secara teoretis merupakan chipper yang tidak dapat dipecahkan.

Terdapat banyak jenis variasi serangan kriptanalitis, dan dapat diklasifikasikan dalam beberapa cara yang berbeda. Perbedaan yang sama yang diketahui oleh penyerang dan kemampuan yang tersedia. Pada serangan chiperteks saja, kriptanalisis memiliki akses hanya pada chiperteks (kriptosistem modern yang baik biasanya secara efektif kebal terhadap serangan cipherteks). Pada serangan teks yang diketahui, kriptanalisis memiliki akses pada chiperteks dan teks yang berhubungan (atau pada banyak pasangan). Pada serangan teks yang terpilih, kriptanalisis memilih teks dan mempelajari tekschipper yang berhubungan (mungkin beberapa kali); sebagai contoh, istilah gardeing yang digunakan oleh Inggris selama Perang dunia II. Akhirnya, pada serangan chiperteks yang terpilih, kriptanalisis dapat memilih chiperteks dan belajar teks yang berhubungan.^[4] Penting untuk diketahui, walaupun dengan jumlah yang sangat besar, ialah sering terjadinya kesalahan (umumnya pada desain atau penggunaan protokol kriptografis).

Kriptanalisis cipher kunci-simetris biasanya melibatkan mencari serangan melawan cipher blok atau cipher aliran yang lebih efisien daripada setiap serangan yang dapat melawan cipher sempurna. Sebagai contoh, serangan brute force sederhana melawan DES membutuhkan satu teks yang diketahui dan dekripsi 255, membutuhkan kira-kira setengah dari kunci yang mungkin, untuk mencapai titik kemungkinan mengetahui kunci dapat ditemukan atau tidak. Namun hal ini tidak cukup menjadi jaminan; serangan kriptanalisis linear terhadap DES membutuhkan 243 teks yang diketahui dan kira-kira 243 operasi DES.^[34] Hal ini dianggap sebagai pengembangan dari serangan brute force.

Algoritme kunci-publik didasari pada kesulitan komputasional pada masalah yang beragam. Kesulitan yang paling terkenal ialah [faktorisasi integer](#) (seperti algoritme RSA yang didasari pada masalah yang berhubungan dengan faktor integer), namun masalah [logaritma diskrit](#) juga penting. Banyak kriptanalisis kunci-publik berhubungan dengan algoritme numerikal untuk menyelesaikan masalah komputasional ini, dan beberapa darinya, efisien (contoh dalam waktu pengerjaan). Sebagai contoh, algoritme yang paling dikenal untuk menyelesaikan kriptografi kurva eliptik versi logaritma diskrit sangat menghabiskan banyak waktu ketimbang algoritme yang paling dikenal untuk faktorisasi, paling tidak untuk masalah dengan besar yang lebih kurang sama. Oleh karena itu, segala hal harus sama, untuk mencapai kekuatan menahan serangan yang sama, teknik enkripsi berbasis faktor harus menggunakan kunci yang lebih besar dari teknik kurva eliptik. Untuk alasan ini, kriptosistem kunci-publik yang didasari pada kurva eliptik telah menjadi lebih dikenal sejak penemuannya pada pertengahan

tahun 1990an.

Sementara kriptanalisis menggunakan kelemahan pada algoritme itu sendiri, serangan pada kriptosistem lainnya didasari pada penggunaan dari algoritme pada perangkat yang nyata, yang disebut side-channel attack. Jika kriptanalisis memiliki akses pada, sebagai contoh, jumlah waktu yang dibutuhkan perangkat untuk mengenkripsi jumlah teks atau memberikan laporan kesalahan pada password atau karakter pin, dia mungkin dapat menggunakan serangan waktu untuk memecahkan cipher yang paling tidak tahan pada analisis. Penyerang mungkin juga mempelajari pola dan panjang pesan untuk mendapatkan informasi berharga; hal ini dikenal sebagai analisis trafik[35] dan cukup berguna untuk peringatan serangan. Administrasi kriptosistem yang lemah, seperti mengizinkan kunci yang terlalu pendek, akan membuat setiap sistem menjadi mudah diserang, terlepas dari faktor lainnya. Dan, tentu saja, [teknik sosial](#), dan serangan lain melawan personel yang bekerja dengan kriptosistem atau pesan yang mereka pegang (seperti perampokan, pemerasan, blackmail, espionase, penyiksaan, dll) menjadi serangan yang paling produktif dari semuanya jenis serangan.

File 14 (Jumlah Kata : 86; Kapasitas File : 14KB)

Banyak karya teoritikal kriptografi berkaitan dengan kriptografi sederhana-algoritme dengan sifat kriptografi dasar-dan hubungannya pada masalah kriptografi lainnya. Alat kriptografi yang lebih sulit lalu diciptakan dari kriptografi sederhana ini. Kesederhanaan ini menyediakan sifat yang penting, yang digunakan untuk mengembangkan alat yang lebih kompleks yang disebut kriptosistem atau protokol kriptografi, yang menjamin sifat keamanan level satu atau lebih tinggi. Bagaimanapun, perbedaan antara kriptografi sederhana dan kriptosistem, cukup tipis; sebagai contoh, algoritme RSA kadang disebut kriptosistem, dan kadang sederhana. Contoh tipikal kriptografi sederhana termasuk [fungsi pseudorandom](#), [fungsi satu-arah](#), dll.

File 15 (Jumlah Kata : 273; Kapasitas File : 15KB)

Satu atau lebih kriptografi sederhana sering digunakan untuk mengembangkan algoritme yang lebih kompleks, disebut sistem kriptografi, atau kriptosistem. Kriptosistem (seperti [enkripsi ElGamal](#)) didesain untuk menyediakan fungsi tertentu (seperti enkripsi kunci publik) sembari menjamin sifat keamanan tertentu keamanan (seperti serangan teks-terpilih) seperti pada model oracle acak. Kriptosistem menggunakan sifat kriptografi sederhana utama untuk mendukung sifat keamanan sistem. Tentu saja, karena perbedaan antara kriptosistem dan kriptografi tidak jelas, kriptosistem yang canggih dapat diperoleh dari kombinasi beberapa kriptosistem sederhana. Pada banyak kasus, struktur kriptosistem melibatkan komunikasi maju mundur di antara dua atau lebih kelompok dalam ruangan. (seperti di antara pengirim dari pesan aman dan penerimanya) atau melewati waktu (seperti data yang dilindungi dengan kriptografi). Kriptosistem

yang seperti itu disebut [protokol kriptografi](#).

Beberapa kriptosistem yang terkenal termasuk enkripsi RSA, [tanda tangan Schnorr](#), enkripsi El-Gamal, [PGP](#), dll. Kriptosistem yang lebih rumit melibatkan sistem [uang elektronik](#)[36], sistem tanda-tangan enkripsi, dll. Beberapa kriptosistem teoritikal termasuk sistem pembuktian interaktif,[37] seperti pembuktian pengetahuan-nol],[38] sistem untuk pembagian rahasia,[39][40], dll.

Hingga saat ini, banyak sifat keamanan kriptosistem didemonstrasikan menggunakan teknik empirial atau menggunakan alasan ad hoc. Saat ini, terdapat upaya untuk mengembangkan teknik formal untuk menyelesaikan keamanan kriptosistem; Hal ini secara umum disebut keamanan terbukti. Ide umum dari keamanan terbukti ialah untuk memberikan argumen tentang kesulitan komputasional yang dibutuhkan untuk membahayakan aspek keamanan kriptosistem (dari setiap musuh).

Ilmu yang melihat seberapa baik implementasi dan integrasi kriptografi dalam penerapannya pada perangkat lunak disebut bidang teknik kriptografi dan teknik keamanan.

File 16 (Jumlah Kata : 143; Kapasitas File : 14KB)

Di Inggris, undang-undang Inggris memberikan izin kepada polisi untuk memaksa pelaku mengungkapkan berkas dekripsi atau memberikan password yang melindungi kunci enkripsi. Tidak memberikan kunci merupakan pelanggaran hukum, dan dikenakan hukuman dua hingga lima tahun penjara jika melibatkan keamanan nasional.^[54] Penuntutan yang berhasil telah terjadi di bawah undang-undang ini; pertama, pada tahun 2009,^[55] menghasilkan 13 bulan penjara.^[56] Hukum pemaksaan yang sejenis juga terdapat di Australia, Finlandia, Prancis, dan India memaksa terdakwa untuk memberikan kunci enkripsi atau password selama investigasi kriminal.

Di Amerika Serikat, kasus kriminal Amerika vs Fricosu menunjukkan jika surat perintah dapat memaksa seseorang untuk mengungkapkan kunci enkripsi atau password.^[57] *Elektronik Frontier Foundation* (EFF) memperdebatkan masalah ini atas pelanggaran perlindungan hak asasi manusia berdasarkan Undang-Undang Dasar.^[58] Pada tahun 2002, pengadilan membuat undang-undang, bahwa terdakwa harus membawa perangkat keras yang tak terenkripsi ke persidangan.^[59]

Dalam banyak yuridikasi, status legal pemaksaan seperti ini masih belum jelas.

File 17 (Jumlah Kata : 279; Kapasitas File : 16KB)

Kode Standar Amerika untuk Pertukaran Informasi atau American Standard Code for Information Interchange (ASCII) merupakan suatu standar internasional dalam kode [huruf](#) dan [simbol](#) seperti [Hex](#) dan [Unicode](#) tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan

oleh [komputer](#) dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII sebenarnya memiliki komposisi bilangan [biner](#) sebanyak 7 bit. Namun, ASCII disimpan sebagai sandi 8 bit dengan menambahkan satu angka 0 sebagai bit significant paling tinggi. Bit tambahan ini sering digunakan untuk uji paritas. Karakter control pada ASCII dibedakan menjadi 5 kelompok sesuai dengan penggunaan yaitu berturut-turut meliputi logical communication, Device control, Information separator, Code extension, dan physical communication. Kode ASCII ini banyak dijumpai pada papan ketik (keyboard) computer atau instrument-instrument digital.

Jumlah kode ASCII adalah 255 kode. Kode ASCII 0..127 merupakan kode ASCII untuk manipulasi teks; sedangkan kode ASCII 128..255 merupakan kode ASCII untuk manipulasi grafik. Kode ASCII sendiri dapat dikelompokkan lagi kedalam beberapa bagian:

Kode yang tidak terlihat simbolnya seperti Kode 10(Line Feed), 13(Carriage Return), 8(Tab), 32(Space)

Kode yang terlihat simbolnya seperti abjad (A..Z), numerik (0..9), karakter khusus (~!@#\$\$%^&*()_+?:'"})

Kode yang tidak ada di keyboard namun dapat ditampilkan. Kode ini umumnya untuk kode-kode grafik.

Dalam pengkodean kode ASCII memanfaatkan 8 bit. Pada saat ini kode ASCII telah tergantikan oleh kode UNICODE (Universal Code). UNICODE dalam pengkodeannya memanfaatkan 16 bit sehingga memungkinkan untuk menyimpan kode-kode lainnya seperti kode bahasa Jepang, Cina, Thailand dan sebagainya. Pada papan keyboard, aktifkan numlock, tekan tombol ALT secara bersamaan dengan kode karakter maka akan dihasilkan karakter tertentu. Misalnya: ALT + 44 maka akan muncul karakter koma (.). Mengetahui kode-kode ASCII sangat bermanfaat misalnya untuk membuat karakter-karakter tertentu yang tidak ada di keyboard.

File 18 (Jumlah Kata : 163; Kapasitas File : 15KB)

Kode atau password dalam [komunikasi](#) adalah aturan untuk mengubah suatu [informasi](#) (sebagai contoh, suatu [surat](#), [kata](#), atau [frasa](#)) menjadi bentuk atau representasi lain, yang tidak harus dalam bentuk yang sama. Dalam komunikasi dan [pemrosesan informasi](#), pengkodean atau penyandian (encoding) adalah proses konversi informasi dari suatu sumber (objek) menjadi [data](#), yang selanjutnya dikirimkan ke penerima atau pengamat, seperti pada [sistem pemrosesan data](#). Pengawakodean atau pengawasandian (decoding) adalah proses kebalikannya, yaitu konversi data yang telah dikirimkan oleh sumber menjadi informasi yang dimengerti oleh penerima. [Kodek](#) (codec) adalah penerapan aturan atau [algoritme](#) untuk penyandian dan pengawasandian (sebagai contoh [MP3](#)) yang dapat berupa penerapan paa sisi [perangkat keras](#) maupun [perangkat lunak](#), dan mungkin pula melibatkan [kompresi data](#).

Penyandian adalah proses untuk mengubah [sinyal](#) ke dalam bentuk yang dioptimasi untuk keperluan [transmisi data](#) atau [[penyimpanan data]

Penyandian (bahasa Inggris: encoding) dalam [komunikasi](#) berarti tindakan pemberian arti [simbol](#)-simbol pada pemikiran. Misalnya: memutuskan kata mana yang akan dikatakan atau dituliskan. Proses penyandian adalah tindakan pemilihan simbol-simbol untuk pemikiran [\[1\]](#).

File 19 (Jumlah Kata : 224; Kapasitas File : 15KB)

Komputer adalah alat yang dipakai untuk mengolah [data](#) menurut [prosedur](#) yang telah dirumuskan. Kata computer pada awalnya dipergunakan untuk menggambarkan orang yang perkerjaannya melakukan perhitungan [aritmetika](#), dengan atau tanpa alat bantu, tetapi arti kata ini kemudian dipindahkan kepada mesin itu sendiri. Asal mulanya, pengolahan informasi hampir eksklusif berhubungan dengan masalah aritmetika, tetapi komputer modern dipakai untuk banyak tugas yang tidak berhubungan dengan [matematika](#). Dalam arti seperti itu terdapat alat seperti slide rule, jenis [kalkulator mekanik](#) mulai dari [abakus](#) dan seterusnya, sampai semua komputer [elektronik](#) yang kontemporer. Istilah lebih baik yang cocok untuk arti luas seperti "komputer" adalah "yang mengolah [informasi](#)" atau "[sistem](#) pengolah [informasi](#)." Selama bertahun-tahun sudah ada beberapa arti yang berbeda dalam kata "komputer", dan beberapa kata yang berbeda tersebut sekarang disebut sebagai komputer. Kata computer secara umum pernah dipergunakan untuk mendefiniskan orang yang melakukan perhitungan aritmetika, dengan atau tanpa mesin pembantu. Menurut Barnhart Concise Dictionary of Etymology, kata tersebut digunakan dalam bahasa Inggris pada tahun 1646 sebagai kata untuk "orang yang menghitung" kemudian menjelang 1897 juga digunakan sebagai "alat hitung mekanis". Selama Perang Dunia II kata tersebut menunjuk kepada para pekerja wanita [Amerika Serikat](#) dan [Inggris](#) yang pekerjaannya menghitung jalan artileri perang dengan mesin hitung. [Charles Babbage](#) mendesain salah satu mesin hitung pertama yang disebut mesin analitikal. Selain itu, berbagai alat mesin sederhana seperti slide rule juga sudah dapat dikatakan sebagai komputer.

File 20 (Jumlah Kata : 407; Kapasitas File : 16KB)

Pada awal [sejarah](#), manusia bertukar informasi melalui [bahasa](#). Maka bahasa adalah teknologi, [bahasa](#) memungkinkan seseorang memahami informasi yang disampaikan oleh orang lain tetapi itu tidak bertahan secara lama karena Setelah ucapan itu selesai, maka informasi yang berada di tangan si penerima itu akan dilupakan dan tidak bisa disimpan lama. Selain itu jangkauan [suara](#) juga terbatas. Setelah itu teknologi penyampaian informasi berkembang melalui [gambar](#). Dengan gambar jangkauan informasi bisa lebih jauh. Gambar ini bisa dibawa-bawa dan disampaikan kepada orang lain. Selain itu informasi yang ada akan bertahan lebih lama. Beberapa gambar peninggalan [zaman purba](#) masih ada

sampai sekarang sehingga manusia sekarang dapat (mencoba) memahami informasi yang ingin disampaikan pembuatnya.

Ditemukannya [alfabet](#) dan [angka arabik](#) memudahkan cara penyampaian informasi yang lebih efisien dari cara yang sebelumnya. Suatu gambar yang mewakili suatu peristiwa dibuat dengan kombinasi alfabet, atau dengan penulisan angka, seperti MCMXLIII diganti dengan [1943](#). Teknologi dengan alfabet ini memudahkan dalam penulisan informasi itu.

Kemudian, teknologi percetakan memungkinkan pengiriman informasi lebih cepat lagi. Teknologi elektronik seperti [radio](#), [televisi](#), [komputer](#) mengakibatkan informasi menjadi lebih cepat tersebar di area yang lebih luas dan lebih lama tersimpan.

TI adalah bidang pengelolaan teknologi dan mencakup berbagai bidang yang termasuk tetapi tidak terbatas pada hal-hal seperti proses, [perangkat lunak komputer](#), [sistem informasi](#), [perangkat keras komputer](#), [bahasa program](#), dan data konstruksi. Singkatnya, apa yang membuat data, informasi atau pengetahuan yang dirasakan dalam format visual apapun, melalui setiap mekanisme distribusi multimedia, dianggap bagian dari TI. TI menyediakan bisnis dengan empat set layanan inti untuk membantu menjalankan strategi bisnis: proses bisnis otomatisasi, memberikan informasi, menghubungkan dengan pelanggan, dan alat-alat produktivitas.

TI melakukan berbagai fungsi (TI Disiplin/Kompetensi) dari menginstal [Aplikasi](#) untuk merancang [jaringan komputer](#) dan [basis data](#) informasi. Beberapa tugas yang TI lakukan mungkin termasuk manajemen data, jaringan, rekayasa [perangkat keras komputer](#), basis data dan desain perangkat lunak, serta manajemen dan administrasi sistem secara keseluruhan. Teknologi informasi mulai menyebar lebih jauh dari konvensional [komputer pribadi](#) dan teknologi jaringan, dan lebih ke dalam integrasi teknologi lain seperti penggunaan ponsel, televisi, mobil, dan banyak lagi, yang meningkatkan permintaan untuk pekerjaan .

Pada masa lalu, para (Dewan Akreditasi untuk Engineering dan Teknologi) dan [Asosiasi untuk mesin komputasi](#) telah bekerjasama untuk membentuk akreditasi dan standar kurikulum [\[4\]](#) untuk program degrees di Teknologi Informasi sebagai bidang studi dibandingkan [\[5\]](#) dengan [Ilmu Komputer](#) and [Sistem Informasi](#). SIGITE (Special Interest Group for IT Education)[\[6\]](#) adalah kelompok kerja ACM untuk mendefinisikan standar ini. Pendapatan layanan TI di seluruh dunia sebesar \$ 763.000.000.000 pada tahun 2009.[\[7\]](#)

LAMPIRAN : PENGUJIAN CIPHERTEKS

1 Pengujian File 1

The screenshot shows the dCode website interface for the 'Shift Cipher' tool. The page title is 'SHIFT CIPHER' and it includes a search bar, a 'Successive Shifts Decoder' section, and a 'Similar tools' sidebar. The search results show an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER-S NOT IN LIST A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z'. The 'Successive Shifts Decoder' section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field and a 'Shift type to apply' dropdown menu with options like 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1,2,3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. The 'Similar tools' sidebar lists various cryptographic tools like Caesar Cipher, Vigenere Cipher, Letter Number (A1Z26) A=1, B=2, C=3, etc.

2 Pengujian File 2

The screenshot shows the dCode website interface for the 'Shift Cipher' tool. The page title is 'SHIFT CIPHER' and it includes a search bar, a 'Successive Shifts Decoder' section, and a 'Similar tools' sidebar. The search results show an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER-S NOT IN LIST A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z'. The 'Successive Shifts Decoder' section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field and a 'Shift type to apply' dropdown menu with options like 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1,2,3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. The 'Similar tools' sidebar lists various cryptographic tools like Caesar Cipher, Vigenere Cipher, Letter Number (A1Z26) A=1, B=2, C=3, etc.

3 Pengujian File 3

The screenshot shows the dCode website interface. At the top, there is a search bar with the text "SEARCH A TOOL ON DCODE BY KEYWORDS:" and a "GO" button. Below the search bar, the results section displays an error message: "Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER'S NOT IN LIST A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z". The main content area is titled "SHIFT CIPHER" and includes a "Successive Shifts Decoder" section with various options for shift types and a "Change of shift" section. A sidebar on the right contains a "Summary" section with links to "Successive Shifts Decoder" and "Successive Shifts Encoder", and a "Similar tools" section listing various cryptographic tools like Caesar Cipher, Vigenere Cipher, etc. A Google AdSense banner is visible on the left side of the page.

4 Pengujian File 4

This screenshot is identical to the one above, showing the dCode website interface. It features the same search bar, error message, "SHIFT CIPHER" main content, "Successive Shifts Decoder" section, sidebar with "Summary" and "Similar tools", and the Google AdSense banner. The overall layout and content are consistent with the previous image.

5 Pengujian File 5

The screenshot shows the dCode website's 'SHIFT CIPHER' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section features a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are 'Change of shift' options: 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Support' section with a 'BECOME A PATRON' button. A 'Feedback' link is also visible on the right edge.

6 Pengujian File 6

This screenshot is identical to the one above, showing the dCode website's 'SHIFT CIPHER' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section features a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are 'Change of shift' options: 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Support' section with a 'BECOME A PATRON' button. A 'Feedback' link is also visible on the right edge.

7 Pengujian File 7

The screenshot shows the dCode website interface for the 'SHIFT CIPHER' tool. The page is titled 'SHIFT CIPHER' and is categorized under 'Cryptography' and 'Substitution Cipher'. It features a search bar on the left with the text 'Search for a tool' and a search button. Below the search bar, there is a 'Results' section with an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER'S NOT IN LIST A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z'. The main content area is titled 'Successive Shifts Decoder' and includes a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu, and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. There is also a 'Change of shift' section with options for 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The right sidebar contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', a 'How to encrypt/decrypt using Shift cipher?' section, and a 'Support' section with a 'BECOME A PATRON' button. A 'Feedback' button is also visible on the right side.

8 Pengujian File 8

This screenshot is identical to the one above, showing the dCode website interface for the 'SHIFT CIPHER' tool. The page is titled 'SHIFT CIPHER' and is categorized under 'Cryptography' and 'Substitution Cipher'. It features a search bar on the left with the text 'Search for a tool' and a search button. Below the search bar, there is a 'Results' section with an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER'S NOT IN LIST A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z'. The main content area is titled 'Successive Shifts Decoder' and includes a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu, and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. There is also a 'Change of shift' section with options for 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The right sidebar contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', a 'How to encrypt/decrypt using Shift cipher?' section, and a 'Support' section with a 'BECOME A PATRON' button. A 'Feedback' button is also visible on the right side.

9 Pengujian File 9

The screenshot shows the dCode website interface for the 'SHIFT CIPHER' tool. The main content area is titled 'SHIFT CIPHER' and includes a search bar with the text 'e.g. type random'. Below the search bar, there is a 'Results' section with an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER'S NOT IN LIST A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z'. The 'Successive Shifts Decoder' section is active, showing a grid of characters and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. The 'Change of shift' section has 'AUTOMATIC DETECTION (BRUTEFORCE)' selected. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various cryptographic tools like Caesar Cipher, Vigenere Cipher, and Enigma Machine. A 'Support' section with a 'BECOME A PATRON' button is also visible.

10 Pengujian File 10

This screenshot is identical to the one above, showing the dCode website interface for the 'SHIFT CIPHER' tool. The main content area is titled 'SHIFT CIPHER' and includes a search bar with the text 'e.g. type random'. Below the search bar, there is a 'Results' section with an error message: 'Error ! Sorry :(MULTIPLE SHIFTED CIPHERTEXT CHARACTER'S NOT IN LIST A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z'. The 'Successive Shifts Decoder' section is active, showing a grid of characters and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. The 'Change of shift' section has 'AUTOMATIC DETECTION (BRUTEFORCE)' selected. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various cryptographic tools like Caesar Cipher, Vigenere Cipher, and Enigma Machine. A 'Support' section with a 'BECOME A PATRON' button is also visible. A large watermark from Universitas Islam Sumatera Utara is overlaid on the page.

11 Pengujian File 11

SHIFT CIPHER
Cryptography > Substitution Cipher > Shift Cipher

Version Française

Summary

- Successive Shifts Decoder
- Successive Shifts Encoder
- How to encrypt using Shift cipher?
- How to decrypt using Shift cipher?

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type random GO

Results

Error ! Sorry :(

MULTIPLE SHIFTED CIPHERTEXT
CHARACTER'S NOT IN LIST
A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

Google AdSense

Monetize your site
With ads you can count on

Learn More

Shift Cipher - dCode
Tag(s) : Substitution Cipher

dCode and you

Using dCode, you accept cookies for statistic and advertising purposes.

Sponsored ads

Reinvent Impact
with Original HP Toner

Successive Shifts Decoder

MULTIPLE SHIFTED CIPHERTEXT

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift type to apply

- AUTOMATIC DETECTION (BRUTEFORCE)
- SIMPLE SHIFT (CAESAR CODE) OF: 3
- MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP):
1, 2, 3
- PROGRESSIVE SHIFTING (1,2,3,4,...)
- DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)
- ALTERNATE SHIFTING (+N,-N) N= 1

Change of shift

- AUTOMATIC DETECTION (BRUTEFORCE)
- EACH CHARACTER
- EACH WORD
- EVERY N CHARACTERS, N= 3

Similar tools

- Caesar Cipher
- Vigenere Cipher
- Letter Number (A1Z26) A=1, B=2, C=3
- Alphabetical Substitution
- Morse Code
- Binary Code
- ROT Cipher
- Polybius Cipher
- Enigma Machine
- ROT-13 Cipher
- ALL TOOLS

Support

BECOME A PATRON

Share

12 Pengujian File 12

SHIFT CIPHER
Cryptography > Substitution Cipher > Shift Cipher

Version Française

Summary

- Successive Shifts Decoder
- Successive Shifts Encoder
- How to encrypt using Shift cipher?
- How to decrypt using Shift cipher?

Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type random GO

Results

Error ! Sorry :(

MULTIPLE SHIFTED CIPHERTEXT
CHARACTER'S NOT IN LIST
A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z

Google AdSense

Monetize your site
With ads you can count on

Learn More

Shift Cipher - dCode
Tag(s) : Substitution Cipher

dCode and you

Using dCode, you accept cookies for statistic and advertising purposes.

Sponsored ads

Reinvent Impact
with Original HP Toner

Successive Shifts Decoder

MULTIPLE SHIFTED CIPHERTEXT

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift type to apply

- AUTOMATIC DETECTION (BRUTEFORCE)
- SIMPLE SHIFT (CAESAR CODE) OF: 3
- MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP):
1, 2, 3
- PROGRESSIVE SHIFTING (1,2,3,4,...)
- DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)
- ALTERNATE SHIFTING (+N,-N) N= 1

Change of shift

- AUTOMATIC DETECTION (BRUTEFORCE)
- EACH CHARACTER
- EACH WORD
- EVERY N CHARACTERS, N= 3

Similar tools

- Caesar Cipher
- Vigenere Cipher
- Letter Number (A1Z26) A=1, B=2, C=3
- Alphabetical Substitution
- Morse Code
- Binary Code
- ROT Cipher
- Polybius Cipher
- Enigma Machine
- ROT-13 Cipher
- ALL TOOLS

Support

BECOME A PATRON

Share

13 Pengujian File 13

The screenshot shows the dCode website interface for the 'Shift Cipher' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are 'Change of shift' options: 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various cryptographic tools like Caesar Cipher, Vigenere Cipher, and Enigma Machine. A 'Support' section with a 'BECOME A PATRON' button is also visible.

14 Pengujian File 14

This screenshot is identical to the one above, showing the dCode website interface for the 'Shift Cipher' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are 'Change of shift' options: 'AUTOMATIC DETECTION (BRUTEFORCE)', 'EACH CHARACTER', 'EACH WORD', and 'EVERY N CHARACTERS, N= 3'. The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various cryptographic tools like Caesar Cipher, Vigenere Cipher, and Enigma Machine. A 'Support' section with a 'BECOME A PATRON' button is also visible.

15 Pengujian File 15

The screenshot shows the dCode website's 'Shift Cipher' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are options for 'Change of shift'.

The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various other cryptographic tools like 'Caesar Cipher', 'Vigenere Cipher', 'Letter Number (A1Z26) A=1, B=2, C=3', 'Alphabetical Substitution', 'Morse Code', 'Binary Code', 'ROT Cipher', 'Polybius Cipher', 'Enigma Machine', and 'ROT-13 Cipher'. There is also a 'Support' section with a 'BECOME A PATRON' button and a 'Share' section.

16 Pengujian File 16

This screenshot is identical to the one above, showing the dCode website's 'Shift Cipher' tool. The main content area is titled 'SHIFT CIPHER' and includes a 'Successive Shifts Decoder' section. This section has a 'MULTIPLE SHIFTED CIPHERTEXT' input field, an 'ALPHABET' dropdown menu set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and several radio button options for 'Shift type to apply': 'AUTOMATIC DETECTION (BRUTEFORCE)', 'SIMPLE SHIFT (CAESAR CODE) OF: 3', 'MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3', 'PROGRESSIVE SHIFTING (1,2,3,4,...)', 'DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)', and 'ALTERNATE SHIFTING (+N,-N) N= 1'. Below these are options for 'Change of shift'.

The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Similar tools' section listing various other cryptographic tools like 'Caesar Cipher', 'Vigenere Cipher', 'Letter Number (A1Z26) A=1, B=2, C=3', 'Alphabetical Substitution', 'Morse Code', 'Binary Code', 'ROT Cipher', 'Polybius Cipher', 'Enigma Machine', and 'ROT-13 Cipher'. There is also a 'Support' section with a 'BECOME A PATRON' button and a 'Share' section.

17 Pengujian File 17

SHIFT CIPHER
Cryptography > Substitution Cipher > Shift Cipher

Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type random GO

Results
Error ! Sorry :(
MULTIPLE SHIFTED CIPHERTEXT
CHARACTER-S NOT IN LIST
A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z

Google AdSense
Monetize your site
With ads you can count on
Learn More

Shift Cipher - dCode
Tag(s) : Substitution Cipher
dCode and you

Using dCode, you accept cookies for statistic and advertising purposes.

Version Française
Summary
Successive Shifts Decoder
Successive Shifts Encoder
How to encrypt using Shift cipher?
How to decrypt using Shift cipher?

Similar tools
Caesar Cipher
Vigenere Cipher
Letter Number (A1Z26) A=1, B=2, C=3
Alphabetical Substitution
Morse Code
Binary Code
ROT Cipher
Polybius Cipher
Enigma Machine
ROT-13 Cipher
ALL TOOLS

Support
BECOME A PATRON

Share

18 Pengujian File 18

SHIFT CIPHER
Cryptography > Substitution Cipher > Shift Cipher

Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type random GO

Results
Error ! Sorry :(
MULTIPLE SHIFTED CIPHERTEXT
CHARACTER-S NOT IN LIST
A.B.C.D.E.F.G.H.I.J.K.L.M.N.O.P.Q.R.S.T.U.V.W.X.Y.Z

Google AdSense
Monetize your site
With ads you can count on
Learn More

Shift Cipher - dCode
Tag(s) : Substitution Cipher
dCode and you

Using dCode, you accept cookies for statistic and advertising purposes.

Version Française
Summary
Successive Shifts Decoder
Successive Shifts Encoder
How to encrypt using Shift cipher?
How to decrypt using Shift cipher?

Similar tools
Caesar Cipher
Vigenere Cipher
Letter Number (A1Z26) A=1, B=2, C=3
Alphabetical Substitution
Morse Code
Binary Code
ROT Cipher
Polybius Cipher
Enigma Machine
ROT-13 Cipher
ALL TOOLS

Support
BECOME A PATRON

Share

19 Pengujian File 19

The screenshot shows the dCode website interface for the 'SHIFT CIPHER' section. The main content area features a 'Successive Shifts Decoder' tool with the following options:

- Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Shift type to apply:
 - AUTOMATIC DETECTION (BRUTEFORCE)
 - SIMPLE SHIFT (CAESAR CODE) OF: 3
 - MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3
 - PROGRESSIVE SHIFTING (1,2,3,4,...)
 - DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)
 - ALTERNATE SHIFTING (+N,-N) N= 1
- Change of shift:
 - AUTOMATIC DETECTION (BRUTEFORCE)
 - EACH CHARACTER
 - EACH WORD
 - EVERY N CHARACTERS, N= 3

The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Support' section with a 'BECOME A PATRON' button.

20 Pengujian File 20

This screenshot is identical to the one above, showing the dCode website interface for the 'SHIFT CIPHER' section. The main content area features a 'Successive Shifts Decoder' tool with the following options:

- Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Shift type to apply:
 - AUTOMATIC DETECTION (BRUTEFORCE)
 - SIMPLE SHIFT (CAESAR CODE) OF: 3
 - MULTIPLE SHIFTING FOLLOWING THE NUMBER SEQUENCE (IN LOOP): 1, 2, 3
 - PROGRESSIVE SHIFTING (1,2,3,4,...)
 - DEGRESSIVE SHIFTING (-1,-2,-3,-4,...)
 - ALTERNATE SHIFTING (+N,-N) N= 1
- Change of shift:
 - AUTOMATIC DETECTION (BRUTEFORCE)
 - EACH CHARACTER
 - EACH WORD
 - EVERY N CHARACTERS, N= 3

The sidebar on the right contains a 'Summary' section with links to 'Successive Shifts Decoder' and 'Successive Shifts Encoder', and a 'Support' section with a 'BECOME A PATRON' button.