Crittografia end-to-end

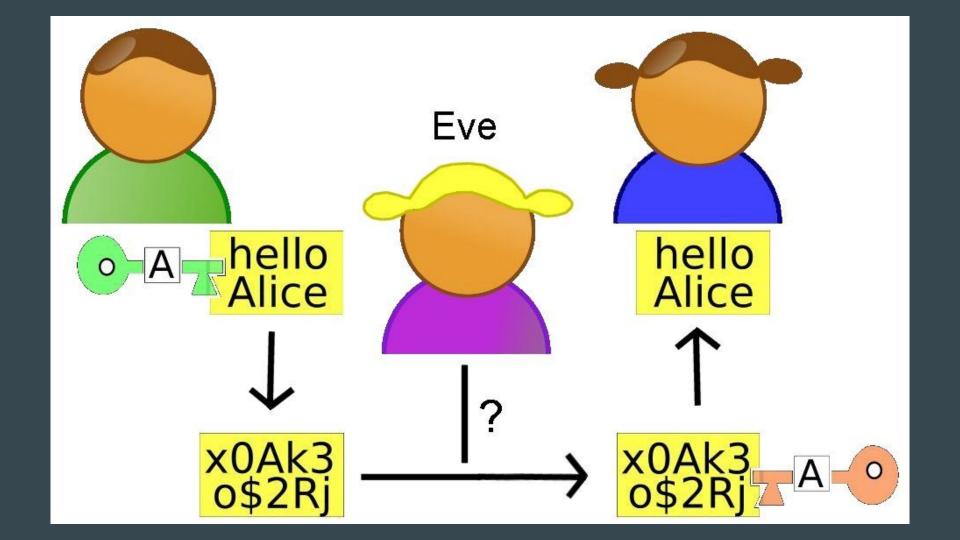
000

Riccardo Serafini Linux Day 2017 - PDP FSUG Fabriano

Crittografia

(dall'unione di due parole greche: κρυπτός [kryptós] che significa "nascosto", e γραφία [graphía] che significa "scrittura")

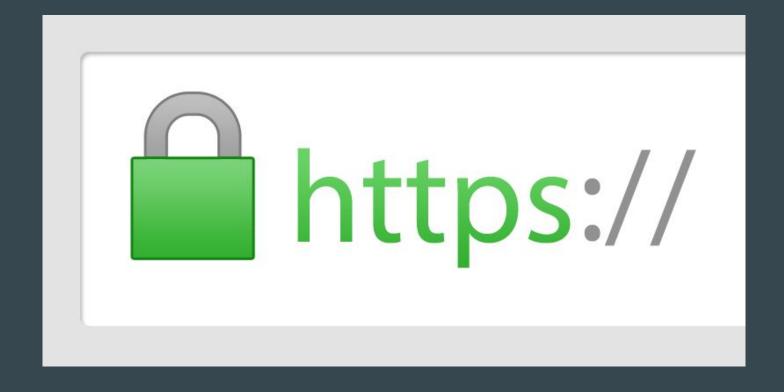
è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.



Enormi numeri primi

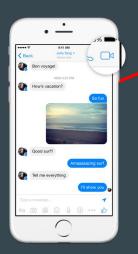
```
D 2D 2D 2D 2D 2D 42 45 47 49 4E 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 2D 49 49 49 45 70 41 49 42 41 41 4B 43 41 51 45 41 ----BEGIN RSA PRIVATE KEY-----.MIJEDAIBAAKCADEA
75 44 58 7A 38 6E 50 72 2F 67 71 67 51 72 55 37 30 46 2B 72 50 42 70 6F 31 55 73 6B 4F 55 6F 77 65 38 58 68 65 4B 69 32 47 58 5A 34 45 65 70 4D uDXz8nPr/gag0ru70F+rPBpo1Usk0Uowe8XheKi2GXZ4EepM
0A 44 49 6D 41 74 61 73 33 41 64 4D 53 4B 4F 58 46 49 30 32 30 34 71 58 45 4A 6C 66 39 57 43 48 2F 42 67 6B 41 71 4E 79 58 39 4C 2F 35 43 6F 35 .DImAtas3AdMSKOXFI0204qXEJlf9WCH/BqkAqNyX9L/5Co5
51 48 78 73 38 50 77 73 43 41 53 33 43 67 37 36 35 0A 47 4F 61 41 61 66 70 67 30 44 72 31 68 44 71 63 55 42 39 75 56 70 34 74 36 44 50 64 6A 77 QHxs8PwsCAS3Cg765.GOaAafpg@Dr1hDgcUB9uVp4t6DPdjw
49 6B 61 6A 79 68 41 7A 32 74 55 53 34 2F 32 66 74 33 52 53 48 33 62 5A 6F 6F 4C 45 4C 6D 41 4B 4D 71 0A 70 4A 48 46 63 75 36 53 41 51 32 72 31 Ikajyhaz2tUS4/2ft3RSH3bZooLELmAKMq.pJHFcu6SAQ2r1
68 55 41 78 38 49 72 67 4E 34 2F 41 41 4B 56 50 41 78 47 55 53 52 47 43 55 62 7A 52 48 46 74 76 56 4C 4A 6E 62 70 59 67 66 42 6D 55 6C 48 4F 65 hUAX8IrqN4/AAKVPAXGUSRGCUbZRHFtvVLJnbpYqfBmUlHOe
64 35 32 0A 4F 46 32 6C 43 36 33 72 6C 44 34 62 6C 67 68 79 34 4D 2F 2F 35 65 77 38 2F 38 37 59 2B 31 61 41 45 75 75 75 42 5A 64 58 32 64 37 47 d52.0F2lC63rlD4blghv4M//5ew8/87Y+1aAEuuuBZdX2d7G
4F 62 48 70 4C 78 52 69 52 32 5A 66 74 61 70 41 48 37 6B 78 0A 51 64 32 77 73 58 53 72 79 78 51 55 44 47 6C 2B 5A 72 46 2F 36 49 48 6B 77 42 62 ObhpLxRix2ZftapAH7kx.0d2wsXSrvxOUDGl+ZrF/6IHkwBb
67 6B 34 70 45 65 74 67 70 65 77 49 44 41 51 41 42 41 6F 49 42 41 41 46 33 6E 49 76 50 31 49 39 66 63 6B 74 56 0A 75 6A 59 38 72 4E 5A 37 74 31 qk4pEetqpewIDAQABAOIBAAF3nIvP1I9fcktV.ujY8rNZ7t1
34 4C 6A 53 78 50 70 50 63 33 61 6B 5A 56 77 61 32 4F 50 67 4B 57 68 53 69 4D 5A 39 51 4B 6D 78 4F 4F 70 4E 52 69 6B 43 46 70 32 77 6A 37 48 51 4LjSxPpPc3akZVwa20PgKWhSiMZ9QKmx00pNRikCFp2wj7HQ
62 5A 4B 4A 46 74 0A 49 2B 54 65 61 58 7A 75 31 4E 38 45 4D 47 32 66 47 4A 42 47 33 55 48 37 53 6E 62 4C 38 49 4B 77 49 44 56 4D 6B 4C 56 48 59 bZKJFt.I+TeaXzu1N8EMG2fGJBG3UH7SnbL8IKWIDVMkLVHY
30 49 46 56 6A 4E 4A 62 44 6C 50 4A 73 66 56 31 72 50 45 78 66 7A 2F 0A 6E 56 36 6A 51 50 30 50 6E 72 50 49 31 49 56 64 39 57 4D 39 6C 41 54 78 0IFV]NJbDlPJsfV1rPExfZ/.nV6j0P0PnrPI1IVd9WM9lATX
64 32 52 79 32 48 6E 7A 46 7A 57 33 59 66 62 59 4D 53 78 58 65 49 73 34 6A 65 38 56 70 6E 58 6D 4A 54 66 79 4E 5A 2F 58 0A 48 47 6E 34 51 7A 35 d2Ry2HnzFzW3YfbYM5xXeIs4je8VpnXmJTfyNZ/X.HGn4Qz5
45 55 6F 64 2B 4D 37 2F 2F 44 50 4B 41 71 4D 32 79 6E 48 44 49 7A 52 57 35 41 68 4F 6F 57 64 30 6F 68 75 32 4C 36 45 67 4D 68 53 49 47 46 6A 48 EUOd+M7//DPKAgM2ynHDIZRW5AhOoWd0ohu2L6EgMhSIGFiH
77 53 61 51 35 4B 31 34 45 0A 66 43 56 73 57 64 79 6D 42 4B 68 45 63 67 46 6B 34 4E 70 69 41 69 65 49 44 62 30 4E 45 76 41 6F 65 50 67 6D 76 79 wSaQ5K14E.fCVsWdymBKhEcgFk4NpiAieIDb0NEVAoePgmvy
47 6B 6E 56 6B 78 44 53 33 37 4D 46 77 75 67 36 4F 76 4B 68 72 39 6E 4B 45 34 0A 32 54 35 67 7A 58 45 43 67 59 45 41 39 56 4C 73 50 32 52 6C 62 GknVkxDS37MFwuq60vKhr9nKE4.2T5qzXECqYEA9VLsP2Rlb
74 74 77 7A 74 6E 5A 69 6D 36 34 49 77 42 57 76 69 5A 38 72 56 75 55 43 59 62 76 33 4C 61 70 5A 4F 30 30 4F 76 48 56 46 42 51 79 0A 49 31 46 4B ttwztnZim64IwBwviZ8rVuUCYbv3LapZ0000vHVFB0y.I1FK
57 50 41 5A 74 39 4B 4D 33 76 66 72 57 55 4D 48 56 67 38 54 57 53 6D 4F 70 77 36 6D 36 53 37 7A 4D 78 2F 78 36 6B 50 78 67 55 37 6B 59 77 38 70 WPAZt9KM3vfrWUMHVg8TWSmOpw6m6S7ZMX/X6KPXQU7kYw8p
75 62 68 68 63 32 6C 73 68 58 6A 66 0A 32 68 56 42 44 65 36 6A 43 68 39 63 64 6B 45 4D 49 76 4C 4F 57 73 31 35 2F 2B 30 52 47 6B 49 37 58 2F 50 ubhhc2lshXjf.2hVBDe6jCh9cdkEMIvL0Ws15/+0RGkI7X/P
43 59 71 75 35 67 31 66 72 50 68 78 2B 78 66 35 74 79 4C 55 43 67 59 45 41 77 44 6F 76 0A 2B 5A 46 4B 35 71 6F 4D 39 4F 6F 54 56 42 46 39 70 67 CYQU5Q1FrPhx+xF5tyLUCQYEAWDOV.+ZFK5Q0M900TVBF9pq
78 49 56 77 50 46 45 52 74 6B 38 71 76 73 4F 66 34 78 73 77 37 75 78 69 55 69 48 62 74 65 39 66 64 4D 44 43 56 41 69 33 77 33 77 69 48 49 0A 44 xIVwPFERtk8avsOf4xs7suxiUiHbte9fdMDCVAi3w3wiHI.D
65 74 52 6F 35 52 78 56 5A 47 43 61 37 6B 43 7A 43 41 5A 67 54 78 73 54 6F 39 55 4F 61 71 4F 65 6A 31 69 4C 71 6C 33 38 77 4D 49 4D 43 68 62 51 etRo5RxVZGCa7kcZCAZqTxsTo9U0aq0ej1iLql38wMIMChb0
58 78 33 32 50 78 32 4E 4B 31 79 46 63 56 32 0A 6A 6E 35 48 6D 47 57 54 4D 6C 5A 31 6A 57 50 39 34 2B 67 30 31 34 41 52 45 4F 62 57 66 4D 69 31 XX32PX2NK1yFcV2.jn5HmGWTMlZ1jWP94+q014ARE0bWfMl1
37 71 35 71 64 32 38 43 67 59 45 41 6A 6E 6B 72 4A 53 47 38 57 75 5A 73 6E 47 55 65 6C 75 76 34 0A 57 72 4E 2B 72 51 34 54 43 47 63 51 45 58 78 7q5qd28CgYEAjnkrJSG8WuZsnGUeluv4.WrN+rQ4TCGcQEXx
   58 31 42 69 44 6E 42 49 44 68 65 57 68 51 4F 35 6E 70 4D 2B 56 32 71 52 74 52 55 39 70 4E 78 63 76 55 6C 56 51 47 43 65 2F 77 42 49 6A 62 4C hXiBiDnBiDheWhQO5npM+V2qRtRU9pNxcvUlVQcCe/wBijbl
50 0A 73 73 73 47 69 4F 46 37 6B 47 38 48 47 65 37 6B 61 72 64 4B 70 30 5A 79 71 69 46 47 32 6A 6B 35 34 43 44 4A 32 44 71 49 53 33 2B 74 4A 69 P.sssGiOF7kG8hCe7kardKp0ZyqiFG2jk54CD)2DqIS3+tJi
78 65 7A 51 6B 77 57 4D 48 4F 6F 5A 68 66 66 31 32 4A 0A 75 41 38 4D 44 46 76 6F 38 47 4F 6D 42 6A 74 73 55 4C 61 54 73 61 55 43 67 59 41 65 69 xez0kwWMH0oZhff12J.uA8MDFvo8GOmBitsULaTsaUCqYAei
36 42 2F 2B 64 52 37 48 74 35 38 4E 49 33 70 74 2F 58 4E 59 76 70 44 79 58 65 52 4A 6C 63 2B 4D 49 2B 54 0A 44 34 39 36 54 65 34 36 30 6A 2B 2F 6B/+dR7Ht58NI3pt/XNYvpDvXeRJlc+MI+T.D496Te4601+,
6C 62 79 62 50 54 61 36 58 31 6B 49 55 53 37 54 44 47 63 72 76 77 37 7A 2F 57 79 63 2B 6B 68 4E 4D 64 4C 39 2B 4D 50 55 77 33 4D 36 63 4A 41 6A \text{lbybPTa6X1kIUS7TDGcrvw7z/Wyc+khNMdL9+MPUW3M6cJA}
73 62 52 2B 0A 50 43 37 54 31 31 34 57 49 59 38 31 68 39 51 6F 62 63 7A 6C 6B 41 69 41 69 6D 63 73 69 6E 6F 79 58 6D 4B 6D 46 73 33 7A 47 38 59 sbr+.PC7T114WIY81h9QobczlkaiaimcsinoyXmKmFs3zG8Y
47 4E 37 4E 71 65 63 57 62 30 4E 2F 6C 58 61 6B 4C 6E 79 45 35 0A 30 6B 46 63 78 51 4B 42 67 51 44 4A 70 45 56 6D 48 31 78 61 32 6C 6A 75 64 4D GN7NqecWb0N/lXakLnyE5.0kFcxQKBgQDJpEVmH1xa2ljudM
63 37 73 61 39 36 34 32 6B 5A 71 35 42 76 79 4B 77 35 44 4C 55 63 43 55 67 59 6F 4F 4E 74 78 34 37 47 62 75 53 36 0A 54 30 73 6D 54 65 4F c7sa9642kZq5BvvKw5DLUcCUqYoONtx47GbuS6.T0T0smTe0
6A 79 6C 64 4E 67 30 72 68 46 4D 71 30 46 69 43 46 76 45 6B 4B 33 66 30 2B 4E 77 44 35 4E 37 51 74 59 31 58 50 6D 54 49 39 6B 71 4F 6C 38 4A 71 ivldng0rhFMg0FiCFvEkK3f0+NwD5N70tY1XPmTI9kg0l8Jg
4C 31 41 39 48 61 6B 0A 38 66 66 54 47 42 48 52 6F 59 62 4E 51 69 7A 44 4D 47 35 57 72 59 4F 75 42 72 77 62 49 52 79 2F 46 57 45 4C 6B 4A 6E 4E L1A9Hak.8fftGBHROYbNQizDMG5WrYOuBrwbIry/FWELkJnN
59 2B 51 49 44 4F 34 76 67 5A 6E 50 59 51 3D 3D 0A 2D 2D 2D 2D 2D 2D 45 4E 44 20 52 53 41 20 50 52 49 56 41 54 45 20 4B 45 59 2D 2D 2D 2D 2D 0A
                                                                                                                                                Y+OIDO4vgZnPYO==.----END RSA PRIVATE KEY----.
```

La utilizziamo tutti i giorni!



Crittografia asimmetrica - modello client/server











Fabrizio Gaias





@fabriziogaias

Amici smanettoni, che vor di'? #WhatsApp

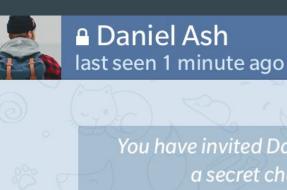
I messaggi che invii in questa chat e le chiamate sono ora protetti con la crittografia end-to-end. Tocca per maggiori informazioni.



Scrivi un messaggio







You have invited Daniel to join a secret chat.

Secret chats:

- Use end-to-end encryption
- Leave no trace on our servers
- Have a self-destruct timer
- Do not allow forwarding

Waiting for Daniel to get online...





Grazie

(per tutto il pesce)

Licenza slide: WTFPL