Security Now! #490 - 01-13-14

The Enigma Machine

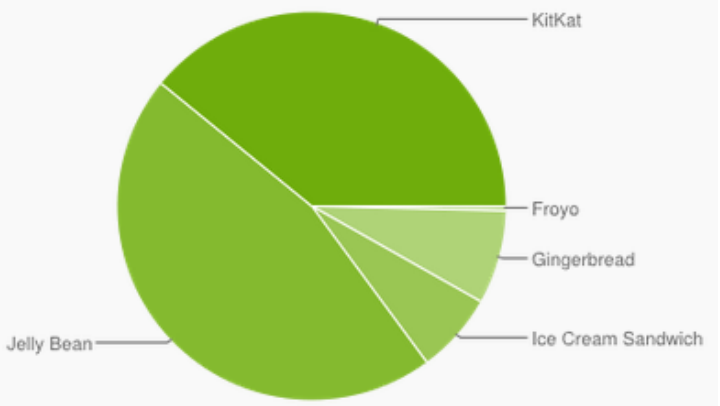
(How it encrypts and how it was cracked)

This week on Security Now!

- Follow-up from last week on CryptoWall, AppLocker & SPDY
- ISPs behavior may be regulated under Title II of the Communications Act.
- SOHO Linux-based routers in botnets
- Windows 7 support status changing TODAY!
- NotePad++ site hacked over the Paris attacks
- Google (again) annoys Microsoft by pre-disclosing details of an unpatched Windows vulnerability… while simultaneously refusing to patch 61% of Android devices.
- U.S. CentCom's Twitter and YouTUBE accounts are hacked,
- And, in the wake of the Paris attacks, British Prime Minister David Cameron proposes outlawing any communications that the government cannot intercept and eavesdrop upon.
- Lots to talk about this week... including... How Enigma encrypts and how it was cracked.

Android OS Version Distribution

Version	Codename	API	Distribution
2.2	Froyo	8	0.4%
2.3.3 - 2.3.7	Gingerbread	10	7.8%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	6.7%
4.1.x	Jelly Bean	16	19.2%
4.2.x		17	20.3%
4.3		18	6.5%
4.4	KitKat	19	39.1%



Security News:

CryptoWall

- Christian Alexandrov (@Diabolikkant)
- Non-Admin account can be recovered:
    - if system protection and system restore run on all drives, including shadow copy services, on non-admin account, there is hope.
    - under non-admin account, crypto wall cannot see, delete or alter any shadow copies used by system restore and system protection.
    - remove malware, then login as admin, use the shadow explorer utility to restore previous versions, before infection.
    - access to read modify or delete shadow copies requires full disk access privilege, which non-admin do not have, but admin do have.

Configuring AppLocker in Windows 7

- Nathan Lamonski (@lamnat25)
  @SGgrc: You do not need MS ActiveDirectory / Group policy. For a workgroup machine you can use the local policy editor explained here howtogeek.com/howto/6317/blo…
- http://www.howtogeek.com/howto/6317/block-users-from-using-certain-applications-with-applocker/
- I replied with thanks for the tip, and Nathan replied:
    - @SGgrc: Thanks, I work IT in K12 Education and use Applocker. Love it. It helps with the malware situation big time.
- How-To Geek:
    - "Ensure a Windows PC Never Gets Malware By Whitelisting Applications"
    - Windows "Family Safety" -- like AppLocker but for all editions of Windows.
    - Windows 8 - built in. / Windows 7 - Install from Live Essentials Package
    - Has an unfortunate "Parent/Child" metaphor.
    - Appears to be managed through a webpage in the Microsoft domain?

IE and SPDY:

- http://www.httpvshttps.com/
- (Previously mentioned that SDPY was FF and Chrome only.)
- Internet Explorer 11 added support for SPDY version 3, but not for the Windows 7 version.
- A problem experienced by some users of Windows 8.1 and Internet Explorer 11 is that on initial loading, Google says "Page not found" but on reloading, it is fine. One fix for this is to disable SPDY/3 in Internet Options > Advanced.
- After version 11, IE will drop the support of SPDY, as it will adopt HTTP/2.
- HTTP/2
    - Is binary, instead of textual.
    - Is fully multiplexed, instead of ordered and blocking.
    - Can deliver parallelism over a single connection.
    - Uses header compression to reduce overhead.
    - Allows servers to “push” responses proactively into client caches

ISPs behavior may be regulated under Title II of the Communications Act.

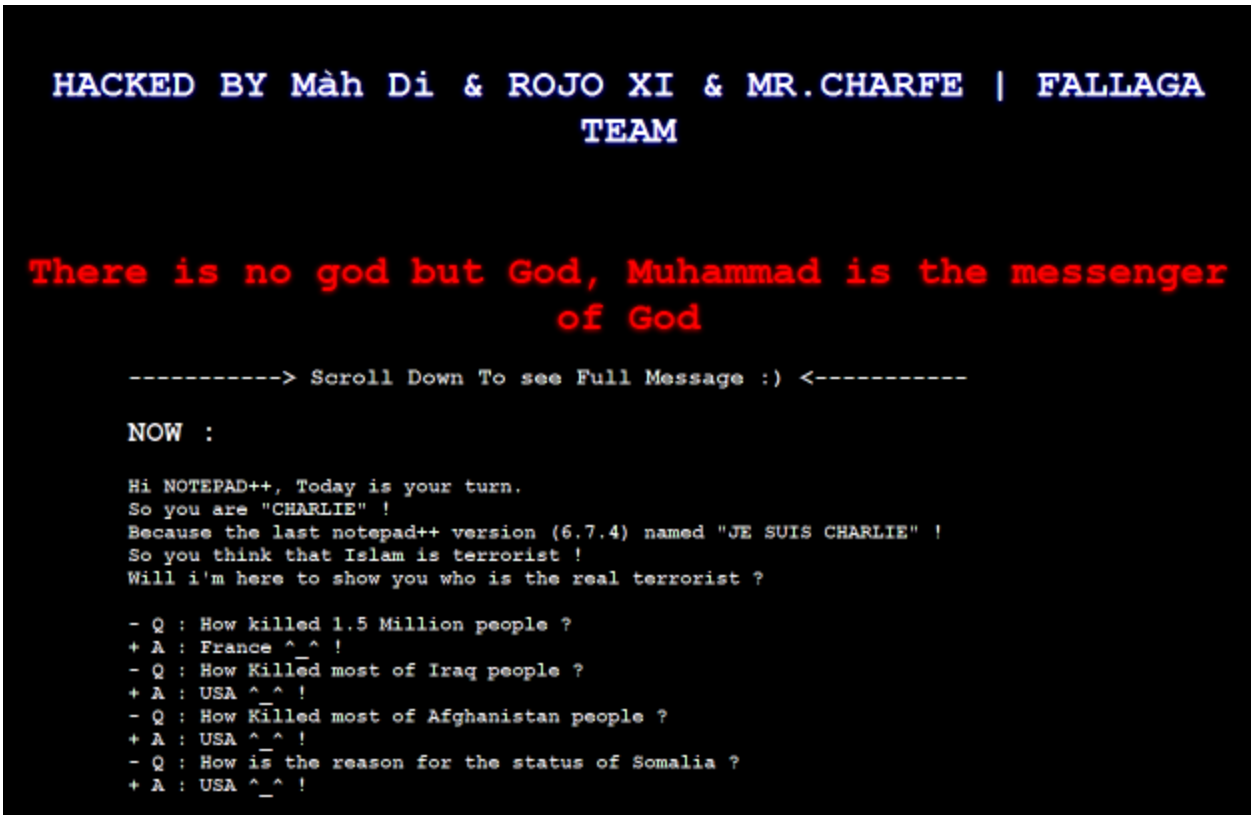
- http://arstechnica.com/business/2015/01/title-ii-for-internet-providers-is-all-but-confirmed-by-fcc-chairman/
- During a one-on-one discussion with Consumer Electronics Association (CEA) President Gary Shapiro, FCC Chairman Tom Wheeler implied that Title II of the Communications Act will be the basis for new net neutrality rules governing the broadband industry. Title II allows the FCC to regulate telecommunications providers as common carriers, and President Obama urged the commission to use Title II to impose net neutrality rules that ban blocking, throttling, and paid prioritization.

Lizard Squad's DDoS network largely powered by SOHO Routers

- Router compromises move from novelty to mainstream.
- Used to attack PSN and Xbox Live over the holidays.
- http://arstechnica.com/security/2015/01/ddos-service-targeting-psn-and-xbox-powered-by-home-internet-routers/
- Linux-based DDoS bot and scanner for other devices.

Notepad++ site hacked

http://notepad-plus-plus.org/



Simon Zerafa brought this to my attention via Twitter
Then Jon M @Liquidretro
@SimonZerafa @SGgrc I downloaded that last night on a new machine.
It was strange... upon first launch it typed out a Charlie message.
v6.7.4 "Je suis Charlie" Edition
http://notepad-plus-plus.org/news/notepad-6.7.4-je-suis-charlie-edition.html

Windows 7 Support Status Changes Tomorrow (Wednesday)

- http://windowsitpro.com/windows-7/clarity-needed-windows-7s-proposed-end-life
- Win7 mainstream support ends 1/13/2015
- EXTENDED support runs through 1/14/2020.
- Losing:
  - No-charge incident support
  - Warranty claims
  - Design changes and feature requests
  - Non-security hotfixes
- Retaining:
  - Paid support (per-incident, per hour, etc.)
  - Security updates
  - Various online support resources

- **Microsoft is again unhappy with Google over pre-releasing news of still-unpatched bug.**
- http://siliconangle.com/blog/2015/01/12/microsoft-unhappy-with-google-again-for-releasing-a-windows-8-1-vulnerability-two-days-before-patch/
- Google's Bug Report:
- https://code.google.com/p/google-security-research/issues/detail?id=123
- Includes Proof-of-Concept batch file.

- Down at the bottom:
  - This bug is subject to a 90 day disclosure deadline. If 90 days elapse without a broadly available patch, then the bug report will automatically become visible to the public.

- Thread conversation dialog:
  - 11 Nov 2014
    - Microsoft confirmed that they are on target to provide fixes for these issues in February 2015. They asked if this would cause a problem with the 90 day deadline.
    - Microsoft were informed that the 90 day deadline is fixed for all vendors and bug classes and so cannot be extended. Further they were informed that the 90 day deadline for this issue expires on the 11th Jan 2015.
  - 11 Dec 2014
    - Microsoft confirmed that they anticipate to provide fixes for these issues in January 2015.
  - 11 Jan 2014 (yesterday)
    - "Deadline exceeded - automatically derestricting"
- Microsoft's not happy about any of this.
  - http://blogs.technet.com/b/msrc/archive/2015/01/11/a-call-for-better-coordinated-vulnerability-disclosure.aspx
  - "A Call for Better Coordinated Vulnerability Disclosure"

Google abandons pre-v4.4 Android Updates

- Extreme Tech: "Google throws nearly a billion Android users under the bus, refuses to patch OS vulnerability" (61%)
- http://mobile.extremetech.com/latest/222540-google-throws-nearly-a-billion-android-users-under-the-bus-refuses-to-patch-os-vulnerability
- Yesterday, the Metasploit hacking kit was updated with 11 exploits effective against Android's WebView browser prior to version 4.4... and Google has clearly stated that it isn't going to fix any of them.
- The whole story is a bit more subtle than that, although it's not yet clear whether that will matter:
- From: Security@Android.com
    - If the affected version [of WebView] is before 4.4, we generally do not develop the patches ourselves, but welcome patches which accompany the report for consideration. Other than notifying OEMs, we will not be able to take action on any report that is affecting versions before 4.4... that are not accompanied by a patch.
- https://community.rapid7.com/community/metasploit/blog/2015/01/11/google-no-longer-provides-patches-for-webview-jelly-bean-and-prior

Centcom's Twitter and YouTube accounts compromised

- U.S. Central Command @CENTCOM · 14 hours ago
  We're back! CENTCOM temporarily suspended its Twitter account after an act of cybervandalism. Read more:
  http://www.centcom.mil/en/news/articles/statement-from-u.s.-central-command-regarding-twitter-youtube-compromise

    - <quote> TAMPA, Fla. - Earlier today, U.S. Central Command's Twitter and YouTube sites were compromised for approximately 30 minutes. These sites reside on commercial, non-Defense Department servers and both sites have been temporarily taken offline while we look into the incident further. CENTCOM's operational military networks were not compromised and there was no operational impact to U.S. Central Command. CENTCOM will restore service to its Twitter and YouTube accounts as quickly as possible. We are viewing this purely as a case of cybervandalism.

David Cameron says new online data laws needed

- Leo: Could you please play this 60-second video into the podcast:
    - https://www.youtube.com/watch?v=u_kqM0gn63M
- "David Cameron says new online data laws needed"
    - http://www.bbc.com/news/uk-politics-30778424
- David Cameron: "We must not allow terrorists safe space to communicate with each other"
- David Cameron has promised a "comprehensive piece of legislation" to close the "safe spaces" used by suspected terrorists to communicate online with each other.
- Speaking at an event in the East Midlands, Mr Cameron said he recognised such powers were "very intrusive" but he believed that they were justified to counter the growing threat to the UK, as long as proper legal safeguards were in place.
- The Independent:
    - http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html
    - "WhatsApp and iMessage could be banned under new surveillance plans"
    - In wake of Paris shootings, Prime Minister wants to ban encryption that government can't read in extreme situations.

SpinRite

Date: Thu, 08 Jan 2015 08:13:05 -0800
From: "JS Cube" via "Shaw" in Canada..

Hello GRC peeps.

This is not a query, but a testimonial. I wanted to leave one on your site, but I couldn't find a link to do so. You may not care, but I 'd like to leave a testimonial anyway.

I had an old but working hard drive that had bad sectors in it, which made it fail any previous attempts to clone it. Your product was my last resort, and it saved me a LOT of time reloading everything into my new SSD. I was able to clone my old hard drive, no problem. (I'm sure you hear this all the time) Thanks!!!

I love your product. It's f@@n' awesome.

Best Regards, JSC

The Enigma Machine

How it encrypts and how it was cracked

History:

- "Cryptography" jumped into the machine age near the end of WWI with the invention of so-called "rotary electro-mechanical enciphering machines."
- Shortly after WWI, a German inventor, Arthur Scherbius, developed and patented a machine for the commercial market. He called his machine: Enigma.
- First Enigma machines were commercially produced by a German inventor.
- Encryption was in the air and "code wheel machines" were simultaneously invented in many other countries.
- The original commercial Enigma $30,000 machine was too expensive for most businesses.
- Germany had been surprised and infuriated to learn that their "unbreakable" codes used during WWI were being routinely cracked and read by everyone.
- So Germany started using Enigmas.
- For Polish Intelligence -- stuck in the middle, bracketed by Russia and Germany -- knowing what was on the minds of both foreign powers was crucial... so they employed the talents of a trio of mathematicians -- probably the first true mathematical cryptanalysts.
- As more and more "Enigma"-encrypted messages began appearing, German communications began going dark.

- They first REVERSE ENGINEERED their own Enigma machines purely from intercepted communications.
- Then THEY invented the first "Bomba" to automate the cracking problem.
- But before long, something else changed, so that even their early machine-enhanced crypto was no longer effective. It had gotten beyond them.
- So just as WWII was breaking out, they transferred their knowledge to British Intelligence and fled Poland.
- Alan Turing and Gordon Welchman designed their own "Bomba" from scratch. It is similar to the previous Polish Bomba only in that they are both rotary electromechanical machines. They worked on entirely different cryptanalytical principles.
- The Polish Bomba relied upon the German practice of transmitting the "per-message" settings of the machine -- twice -- at the beginning of every message. This always made it fragile because the Germans might change that practice at any time... and they did in May of 1940... rendering the Polish designed Bomba useless.
- Poland's cryptographers DID provide the internal wiring of the machine and a proof-of-concept of a functional code breaking machine.

Hardware:

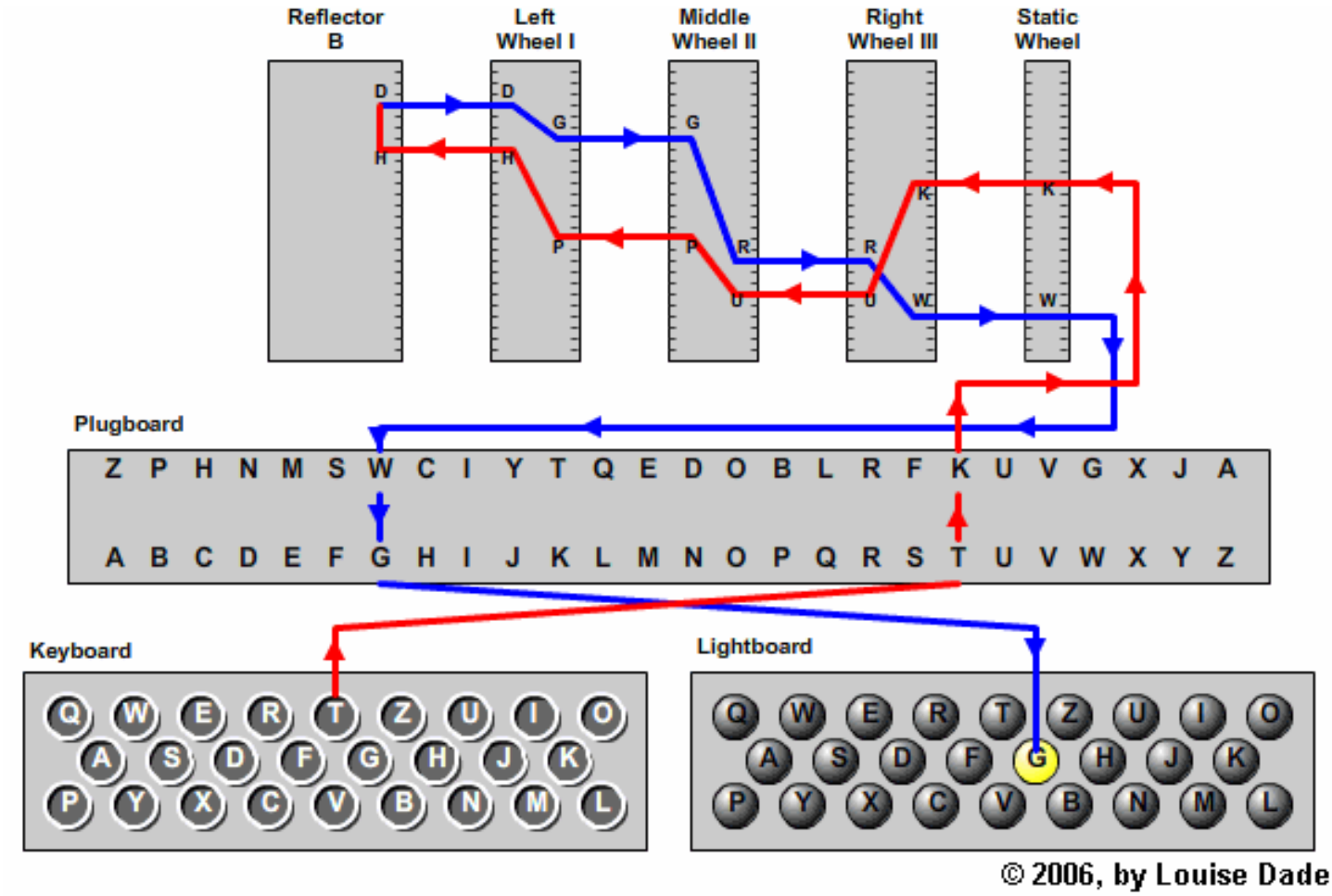
- Keyboard & Lights
  - 26 keys (QWERTZ) and 26 lights
  - No upper or lower case, numbers, punctuation, or space.
  - "X" used as end-of-sentence
  - Numbers were encoded by assigning digits to the top row of keys and prefixing any string of digits with a "Y".

- Rotors
  - 4 inches in diameter - 26 spring-loaded pins on the right, 26 contact pads on the left.
  - Total of 5 (I, II, III, IV, V), choose any three.
  - Can not only each be set to any of 26 positions, but interchanged.
  - Modified Odometer-like motion: "Fast", "Middle" and "Slow" rotors.

- Reflector
  - 26 contacts containing 13 cross-connection wires in a fixed but arbitrary configuration.

- Rings
  - 26-position notched rings which determine when the rotor to the left will be stepped.

- Plugboard
  - 26-positions filled at random by ten connector-terminated cables.
  - Interchanges the connections between the keyboard and lights, and the scrambler system.

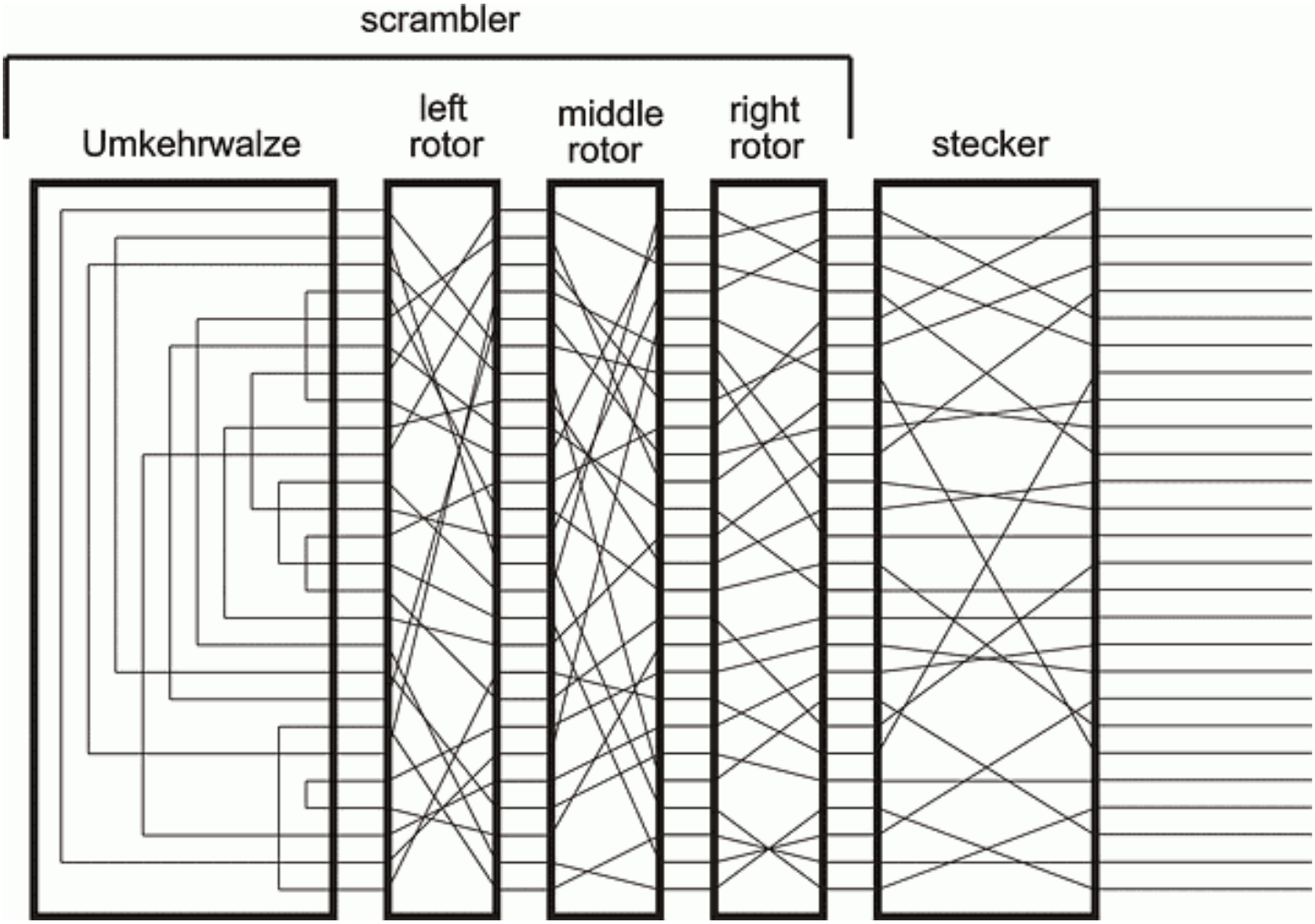


Complexity:

- Rotor choice and arrangement: 5x4x3 = 60
- Ring setting: 26x26 = 676 (righthand rotor's ring had no one to affect.)
- Initial Rotor Settings: 26x26x26 = 17,576
- Plugboard had the largest complexity, over 150,738,274,937,300
- 60 x 17576 x 676 x 1.507382749373 x 10^14 = 1.074586873273 x 10^23
- One Hundred Sextillion - 100,000 Billion Billion
- The task of the cryptanalyst was to determine which *ONE* from among that tremendous number of settings had been chosen FOR THAT DAY.

German Enigma Daily Setup Codebook:

- Rotor order: IV, I, V
- Ring Setting: 23, 02, 17
- Plug Board: AR KT MW LC XD EJ ZB UY PS HN
- Starting Pos: TXM



Protocol:

- Operator
  - Sets machine to the code of the day
  - Per message, chooses three characters at random.
  - Encrypts and sends these three randomly chosen characters TWICE.
  - Sets the machine to the three randomly chosen characters and sends the message.
- Messages are typically broken into groups of four letters.

Weaknesses:

- The repeating three letters allowed the Pols to reverse engineer the machine and build the first Polish bomba. (Germany stopped doing that on May 1st, 1940.)
- "Cribs" : Known plaintext attack (Probably phrase attack)
- Due to the "reflector", no letter can encode to itself.
- Reciprocal "Steckerboard" (plug-board) was a crucial flaw (hugely more contradictions.)

Cracking the Enigma

- The Bomba rapidly tested rotor settings searching for internal contradictions.